Public Document Pack

**STROUD DISTRICT COUNCIL**
Council Offices • Ebley Mill • Ebley Wharf • Stroud • GL5 4UB
Telephone 01453 766321
www.stroud.gov.uk **Email: democratic.services@stroud.gov.uk**

08 April 2024

# AUDIT AND STANDARDS COMMITTEE

A meeting of the Audit and Standards Committee will be held on **TUESDAY, 16 APRIL 2024** in the Council Chamber, Ebley Mill, Ebley Wharf, Stroud at **7.00 pm**

KRO'Leary

Kathy O'Leary
Chief Executive

**Please Note:** The meeting is being held in the Council Chamber at Stroud District Council and will be streamed live on the Council's YouTube Channel. A recording of the meeting will be published onto the Council's website. The whole of the meeting will be recorded except where there are confidential or exempt items, which may need to be considered in the absence of press and public.

If you wish to attend this meeting, please contact democratic.services@stroud.gov.uk.
This is to ensure adequate seating is available in the Council Chamber.

## AGENDA

1. **APOLOGIES**
To receive apologies for absence.

2. **DECLARATION OF INTERESTS**
To receive declarations of interest.

3. **MINUTES (Pages 5 - 12)**
To approve the minutes of the meeting held on 30 January 2024.

4. **PUBLIC QUESTIONS**
The Chair of the Committee will answer questions from members of the public submitted in accordance with the Council's procedures.

**DEADLINE FOR RECEIPT OF QUESTIONS**
**Noon on Wednesday, 10 April 2024**

Questions must be submitted to the Chief Executive, Democratic Services, Ebley Mill, Ebley Wharf, Stroud and can be sent by email to Democratic.services@stroud.gov.uk

5. **MEMBER QUESTIONS**
See Agenda Item 4 for deadlines for submission.

The cost of printing this doc pack: Approx. £22.95 (3 Copies)
The carbon cost of producing this doc pack: Approx. 15.3 tonnes
The cost of posting this doc pack: Approx. £1.21 (each)

6. **INFORMATION GOVERNANCE FRAMEWORK (Pages 13 - 48)**
For Committee to consider the changes to the reviewed and consolidated Information Governance (iGov) Framework (2024-2028).

7. **SAFEGUARDING AUDIT - MANAGEMENT UPDATE (Pages 49 - 52)**
To provide the Committee with an update on the progress made against the management actions to address the recommendations.

8. **EXTERNAL AUDIT UPDATE (Pages 53 - 66)**
To inform Members of the External Audit activity progress.

9. **COUNTER FRAUD AND ANTI-CORRUPTION POLICY (Pages 67 - 86)**
To present the Audit and Standards Committee an updated Counter Fraud and Anti-Corruption Policy for approval and adoption.

10. **COUNTER FRAUD AND ENFORCEMENT UNIT FRAUD RISK STRATEGY (Pages 87 - 110)**
To present the Audit and Standards Committee with a Fraud Risk Strategy, so that they may consider the approach taken by the Counter Fraud Partnership.

To provide assurance to the Audit Committee that the risks of fraud committed against the Council are recognised, managed and mitigated for in accordance with Council priorities, and changing fraud trends.

11. **COUNTER FRAUD AND ENFORCEMENT UNIT REPORT (Pages 111 - 116)**
To provide the Committee with assurance over the counter fraud activities of the Council.

Direct updates will continue to be provided biannually and are presented detailing progress and results for consideration and comment as the body charged with governance in this area.

The report also provides the annual update in relation to the Regulation of Investigatory Powers Act 2000 (RIPA), the Investigatory Powers Act 2016 (IPA) and the Council’s existing authorisation arrangements.

12. **TREASURY MANAGEMENT Q3 REPORT (Pages 117 - 128)**
To provide an update on treasury management activity as at 31/12/2023.

13. **DRAFT 2024-25 INTERNAL AUDIT PLAN (Pages 129 - 136)**
To provide the Committee with a summary of the draft Risk Based Internal Audit Plan 2023-24, as required by the Accounts and Audit Regulations 2015 and the Public Sector Internal Audit Standards (PSIAS) 2017.

14. **UPDATE ON ANNUAL GOVERNANCE STATEMENT ACTION PLAN (Pages 137 - 142)**
This report gives an update on the areas of focus identified for 2023/34 in the Annual Governance Statement 2022/23.

15. **STANDING ITEMS**
(a) **Corporate Risk Register Update (Pages 143 - 152)**
(b) **To consider the Work Programme (Pages 153 - 154)**

16. **INTERNAL AUDIT PROGRESS UPDATE REPORT 2023-24 (Pages 155 - 170)**

To inform Members of the Internal Audit activity progress in relation to the approved Internal Audit Plan 2023-24.

## Members of Audit and Standards Committee

| | |
|---|---|
| **Councillor Nigel Studdert-Kennedy (Chair)** | **Councillor Martin Pearcy (Vice-Chair)** |
| Councillor Paula Baker | Councillor Nick Hurst |
| Councillor Martin Brown | Councillor Christopher Jockel |
| Councillor Doina Cornell | Councillor Keith Pearson |
| Councillor Laurie Davies | Councillor Ashley Smith |
| Councillor Stephen Davies | |

This page is intentionally left blank

Agenda Item 3

2023/24

STROUD DISTRICT COUNCIL
Council Offices • Ebley Mill • Ebley Wharf • Stroud • GL5 4UB
Tel: (01453) 754 351/754 321
www.stroud.gov.uk Email: democratic.services@stroud.gov.uk

# AUDIT AND STANDARDS COMMITTEE

**Tuesday, 30 January 2024**

**7.00 - 9.16 pm**

**Council Chamber**

## Minutes

**Membership**

**Councillor Nigel Studdert-Kennedy (Chair)**
*Councillor Paula Baker
Councillor Martin Brown
Councillor Doina Cornell
*Councillor Laurie Davies
Councillor Stephen Davies

**Councillor Martin Pearcy (Vice-Chair)**
*Councillor Nick Hurst
Councillor Christopher Jockel
Councillor Keith Pearson
*Councillor Ashley Smith

*Absent

**Officers in Attendance**

Strategic Director of Resources
Corporate Director (Monitoring Officer)
Head of Audit Risk Assurance (ARA)
Principal Auditor
Accountancy Manager
Principal Accountant
Head of Service Counter Fraud and Enforcement Unit
Deloitte
Senior Policy and Governance Officer
Democratic Services & Elections Officer

### ASC.017 Apologies

Apologies for absence were received from Councillors Baker, Hurst, Laurie Davies and Smith.

### ASC.018 Declaration of Interests

There were none.

### ASC.019 Minutes

**RESOLVED That the Minutes and the exempt minutes of the meeting held on 26 September were approved as a correct record.**

### ASC.020 Public Questions

There were none.

### ASC.021 Member Questions

There were none.

**ASC.022 Contract Management Framework Update**

The Senior Policy and Governance Officer introduced the report and highlighted a small error where it stated that the Procurement Strategy was awaiting approval. It had been approved at the Strategy and Resources Committee in November 2023. She explained that the report was an annual report which included updates, a summary of the audit recommendations and the management response. The updates and changes to the original report had been highlighted throughout the appendices and the main changes were:

- Levels of contract management (high, medium and low) had now been defined within the framework.
- More information regarding risk management had been included.
- Approval from the Head of Service for the Contract Plan was now required.
- The level of the mandatory contract management plan had been increased from £25k – £75k which was now in line with the financial thresholds.

The Senior Policy and Governance Officer highlighted following key points:

- The second line of defence activity took place on a quarterly basis by the Policy and Governance Team.
- The Procurement Strategy included an annual action plan which referenced the framework.
- The Procurement Act was due to come into effect in October 2024 which would affect the Procurement and Procedure Rules. Therefore they would likely need to come back to the Committee for approval.
- Training for Officers would begin in February and Members would receive training as part of the induction programme following the elections in May.

In response to Councillor Pearson, it was confirmed that the changes would not take effect until after the report had been approved.

Following a question from the Chair, the Senior Policy and Governance Officer explained that there were several notices that would need to be published following approval, which would all be publicly available on the website.

Councillor Pearcy asked whether the system had been updated to reflect the requirements for a more transparent process as part of the upcoming legislation. The Senior Policy and Governance Officer confirmed that the system already had that capability.

Councillor Davies raised concerns regarding training fatigue. The Senior Policy and Governance Officer explained that there would be initial training sessions for all Officers and then further refresher sessions to provide information on any amendments later in the year.

Councillor Cornell raised a question regarding a further piece of legislation which could restrict future procurement investments. The Senior Policy and Governance Officer confirmed that the Procurement Strategy would set out the framework for the next 5 years and there were no impacts expected.

In response to Councillor Jockel, The Senior Policy and Governance Officer confirmed that the Social Value Policy had been adopted in 2021 and they were working to ensure that the contract management framework reflected any existing policies.

Councillor Pearcy asked where the responsibility of risk sat within a contract agreement. The Senior Policy and Governance Officer explained discussions took place before the signing of a contract to ensure both parties were aware of their responsibilities and these should be reviewed throughout the duration of a contract at regular meetings.

The Chair questioned what the process was if a contract was not progressing as expected. The Senior Policy and Governance Officer explained it would be discussed at the Community Governance Group and then reported to the Strategic Leadership Team for review. If a serious failure was identified it would then be escalated to Committee or Internal Audit as appropriate.

Councillor Pearson commended the Officers.

Councillor Pearson proposed and Councillor Pearcy seconded.

After being put to a vote, the Motion was carried unanimously.

**RESOLVED To approve the updated Contract Management Framework**

## ASC.023 Annual Audit Letter

Michelle Hopton from Deloitte introduced the report and explained that it included an update for both the 2021/22 and the 2022/23 audit as summarised below.

2021/22

- There were national issues regarding the pension fund which had led to a delay with the 2022 audit opinion being signed. These had now been resolved and the FY 2022 audit had been signed off.

2022/23

- The audit was in its final stages to resolve any remaining queries with the aim of signing off the accounts at the end of March 2024.
- They were also looking to complete a value for money piece of work.
- They would be looking to bring back a further final report which summarised all of the updates regarding both 2021/22 and 2022/23 audits. It was hoped that this would be ready for the next Audit and Standards Committee meeting.
- Pages 68-69 of the report detailed the corrected misstatements identified and there was one uncorrected misstatement which was detailed on page 70.

Councillors were given the opportunity to ask the Officers questions, the following responses were given:

- They had amended how they the presented their report to further increase transparency.
- A judgemental misstatement was based on an estimation and therefore was subjective to a point compared to a factual misstatement which was factually wrong. A small judgemental misstatement would not be a material consideration however anything that was large enough to become material was feedback to management to decide whether to adjust the amount.
- The Section 151 Officer had the final say on what figures went into the account however it was very unlikely that he would input any figures that audit were not in agreement with.
- There were national issues regarding the sign off of Local Authority audits which had created a backlog with hundreds of accounts still awaiting sign off. The 2022/23 accounts had already passed the initial deadline and a new backlog deadline had been put in proposed by Central Government for the end of September 2024.

The Strategic Director of Resources confirmed to the Committee that despite the backlog, Stroud District Council had met its earlier deadline to publish its draft accounts.

Councillor Jockel raised a query regarding the fixed assets valuation. The Strategic Director of Resources explained that it was an area of judgement with large sums which meant that it was more frequently challenged. He further explained the actions they had taken to address this such as:

- Increased the number of assets to be valued each year.
- Improved the asset register system for recording depreciation in valuations.
- Utilised updated property valuations.

**RESOLVED To note the annual audit letter on 2022/23 external audit.**

## ASC.024 COUNTER FRAUD AND ENFORCEMENT UNIT REPORT

The Head of Service, Counter Fraud and Enforcement Unit (CFEU) introduced the report and briefly summarised its contents. The report included an update on the work surrounding the Council Tax reduction scheme, National Fraud Initiative (NFI) match information, Revenue and Benefit single discount review matches, housing and tenancy fraud referrals and further details of other fraud investigative activities.

The Head of Service CFEU explained that due to Stroud becoming a full partner with the Counter Fraud and Enforcement Team there would be additional reports for Committee to consider in April.

In response to Councillor Cornell, the Head of Service CFEU confirmed that it was a shared service. They were employed by Cotswold District Council and seconded out to all other councils in the partnership. After a further question from Councillor Cornell the Head of Service CFEU confirmed there were other councils within the partnership who also had their own housing stock.

Councillors received the following answers in response to their questions asked:

- The financial loss avoidance had been highlighted as per a request received at a previous Committee.
- The Council Tax single persons had returned a high number of matches. A match meant that there was a discrepancy with the information provided.
- There were a number of reasons other than fraud that contributed to the high number of Council Tax matches.
- Training sessions for Members regarding the CFEU partnership would be rolled out after April.
- There was a specific addendum on the website relating to the NFI investigations and for further information for the public.

Councillor Davies commended the report.

**RESOLVED To consider the report and comment as necessary.**

## ASC.025 Half year Treasury Management report 2023/24

The Principal Accountant introduced the report and provided a brief overview which included:

- Table 1 on page 85 outlined the half year interest earned on treasury investments which was £1.286m.

- Table 3 on page 86 was a snapshot of investments with their ESG rating. The lowest of which had since been redeemed.
- Table 4 on page 87 detailed the return on specified investments.
- Page 87 detailed the termination date for the Lothbury Property Fund investment which had been extended.
- Page 89 highlighted the Camdor training which was postponed and would need to be rescheduled potentially following the May elections.

Councillor Davies queried the Lothbury Property Fund and the Principal Accountant explained that the fund was frozen until 31 March 2024. There was a potential for a merged fund proposal which would allow for the council to stay invested with the property fund should they wish. However if that proposal did not come forward or the council was not minded to continue its investment then it would be re-paid at it's current value.

Councillor Davies questioned the current value of the fund and whether it had depreciated. The Principal Accountant explained that it had and was continuing to decrease.

The Strategic Director of Resources clarified that where investments had returned higher than expected, not all of the additional income had been spent. They had an investment risk reserve with approximately £820k. He then explained the disinvestment process to the Committee should the Lothbury Property Fund not continue.

Councillor Davies questioned whether there were any other investments that significantly depreciated. The Principal Accountant explained that the investment values fluctuated and could be found with their initial investment figure in table 2 on page 85.

Councillor Pearson clarified that although the initial investment had depreciated, they had received a higher value of returns.

In response to Councillor Pearcy, the Principal Accountant confirmed that the Lothbury Property Fund consisted of real assets which would need to either be sold to pay back initial investments or transferred to a large Property Fund in the case of a merge.

Councillor Pearson proposed and Councillor Pearcy seconded.

After being put to a vote, the Motion was carried unanimously.

**RESOLVED To accept the Treasury Management half year report.**

## ASC.026 Treasury Management Strategy 24/25

The Principal Accountant provided a summary of the report including a brief outline of its appendices. He highlighted table 2 on page 102 which outlined the councils Capital spending plans and table 3 detailed the debt repayment plans. The liability benchmark, which was a relatively new indicator, could be found at page 103.

Councillor Cornell raised a question regarding the ethical investment policy and current legislation that Central Government were discussing and whether it would have an impact. The Strategic Director of Resources clarified that the Government were discussing the Economic Activities of Public Bodies (Overseas Matters) Bill in the House of Commons. He further explained that its intention was to prevent Local Authorities from making individual decisions to not invest or procure from particular nation states with the exception of Russia and Belarus and it was not believed to have an impact. If the bill was passed, they would ensure that they were complying and bring any urgent matters to Committee where required.

The Chair questioned whether 20% of the revenue of housing was set aside to re-pay interest on debt. The Accountancy Manager confirmed that there was considerable debt within the Housing Revenue Account (HRA) due to its self-financing decision in 2012. There was additional borrowing for new builds and major works which would be continued to fund the retrofit programme, sustainable energy works and additional properties. There was an annual contribution and an earmarked reserves for the repayment of debt and it was a longer-term borrowing.

Councillor Pearson asked whether the data could be extracted to see the benefits of being self-financed. The Accountancy Manager explained that it would be very difficult to calculate due to many different factors.

In response to Councillor Davies question about the self-financing debt being written off for councils who utilised housing associations, the Accountancy Manager explained that there were many financial differences between councils and housing associations and how the paid VAT. She confirmed that the debt would not be there had the decision been made to not retain the housing stock.

Councillor Pearcy asked a question regarding the sensitivity of interest rates against investments. The Principal Accountant confirmed that the majority of borrowing was completed on a fixed rate.

Councillor Pearson proposed and Councillor Pearcy seconded.

After being put to a vote, the Motion was carried unanimously.

**RECOMMENDED THAT COUNCIL**

a) **adopt the prudential indicators and limits for 2024/25 to 2026/27;**
b) **approve the Treasury Management Strategy 2024/25, and the treasury prudential indicators;**
c) **approve the Investment Strategy 2024/25, and the detailed criteria for specified and non-specified investments**
d) **approve the MRP Statement 2024/25; and**
e) **approve the Ethical Investment Policy**

## ASC.027 Update on Annual Governance Statement Action Plan

The Corporate Director (Monitoring Officer) introduced the report and explained that it was an update on the progress against the action plan found at appendix 1 on page 137. She highlighted that a few of the target dates had been amended due to resources and that a number of the actions had been completed and a significant amount of work had been undertaken for those still outstanding.

The Corporate Director (Monitoring Officer) gave the following answers in response to Councillors:

- Page 138 showed ‘ongoing’ in the update section. She explained that there was a lot of work taking place in the background to set up the correct tools in order to progress the actions.
- The Risk Management deadlines had been amended due to a delay with the report going to Committee which in turn had delayed the other actions under that heading.

Councillor Davies commended Ideagen and requested further detail to be included within the system for Councillors to see the breakdown of progress.

In response to Councillor Schoemaker, The Corporate Director (Monitoring Officer) confirmed that there was a collaborative approach used to identify deadlines with Officers.

Councillor Pearcy asked if this could be assessed again in April instead of July as per the work programme.

The Corporate Director (Monitoring Officer) agreed to bring an additional report back to the Committee.

**RESOLVED To note the progress made against the Annual Governance Statement action plan.**

## ASC.028 Internal Audit Progress Update Report

The Head of Audit Risk Assurance (ARA) introduced the report and provided a brief overview. He informed the Committee that all of the activities were of a substantial or acceptable level of assurance.

Councillor Jockel asked how the risk for the Canal Restoration Project was identified. The Principal Auditor explained that the audit focused on the procedures and controls in place for the project's risk management and was completed through discussion with lead officers & review of audit trail. In response to a further question from Councillor Jockel, she clarified that audit activities were carried out according to the scope agreed in the Committee approved audit plan. The Head of ARA confirmed that the scope was also defined in the audit terms of reference. If the audit identified an issue/risk outside of the audit scope, the item would be reviewed with Officers to ensure awareness and appropriate action.

Councillor Pearcy raised concerns with the safeguarding framework audit and requested an update at the next Committee meeting. The Principal Auditor explained that ARA would not be able to provide a follow up audit update based on the requested timing, however they could arrange for a management update.

The Corporate Director (Monitoring Officer) confirmed that as part of the Corporate Governance Group discussions, they were looking to input all audit recommendations onto Ideagen to better track the progress and completion. The Principal Auditor confirmed that the first update to Committee on audit recommendation monitoring approach will be in July 2024.

Councillor Pearcy queried item 10 on page 160 which had a status of 'planned' due to the previous report stating that the draft report had been issued. The Principal Auditor confirmed that the September 2023 Committee report contained an error and should have shown the item as planned.

Councillor Pearson proposed and Councillor Brown seconded.

After being put to a vote, the Motion was carried unanimously.

**RESOLVED To:**

**i. Accept the progress against the Internal Audit Plan 2023-24; and**

ii. **Accept the assurance opinions provided in relation to the effectiveness of the Council's control environment (comprising of risk management, control and governance arrangements)**

## ASC.029 Corporate Risk Register Update

The Strategic Director of Resources introduced the update and gave a brief history to of the reporting of risks to Committee. He explained that previously Members were unable to view the risks due to a technical change and with the introduction of ideagen, Members were now able to view the Strategic Risk Register however it would continue to be reported to the Committee. He highlighted the risks that had been amended and the 3 new risk which had been added as laid out on page 163.

The following answers were given in repose to questions asked by Councillors:

- SR13 had a number of controls in place to manage the risk and therefore it had a lower risk score. This did not mean that it wasn't a sever risk and it was constantly reviewed.
- It was important to look at the Risk Appetite to ensure that it was at the best possible place and that every precaution to manage each risk had been taken. Once the risk had reached an acceptable risk target, it could then be transferred from the Strategic Risk Register.
- SR16 and SR17 were new risks which had not yet had their controls established therefore the risk target could not yet be calculated.
- SR10 was based around not delivering the project as agreed by Members. It would be for Members to decide the tolerance levels for the risk and whether it was something that they could accept should there be any changes which would follow the reporting process through the Committee system.

## ASC.030 To consider the Work Programme

It was agreed earlier in the meeting to move the Annual Governance Statement Update from the July meeting to the April meeting and to include a Management Update to the April meeting for the Safeguarding Audit.

**RESLOVED To note the above updates to the work programme.**

The meeting closed at 9.16 pm

Chair

**STROUD DISTRICT COUNCIL**

**AUDIT AND STANDARDS COMMITTEE**

**TUESDAY, 16 APRIL 2024**

| | | | | |
|---|---|---|---|---|
| **Report Title** | Updated Information Governance Framework | | | |
| **Purpose of Report** | For Committee to consider the changes to the reviewed and consolidated Information Governance (iGov) Framework (2024-2028). | | | |
| **Decision(s)** | **The Committee RESOLVES to:**<br>**a) Approve the revised Information Governance Framework; and**<br>**b) Delegate responsibility to the Data Protection Officer to make minor changes to the Information Governance Framework.** | | | |
| **Consultation and Feedback** | Counter Fraud and Enforcement Unit – Surveillance policy wording<br>Policy & Governance team – Accessibility and editing | | | |
| **Report Author** | Owen Chandler, Information Governance Officer<br>Email: owen.chandler@stroud.gov.uk | | | |
| **Options** | 1. Accept revised and consolidated framework.<br>2. Revert to individual policies, procedures, and guidance. | | | |
| **Background Papers** | None | | | |
| **Appendices** | 1 - Information Governance Framework 2024 – 2028 | | | |
| **Implications (further details at the end of the report)** | Financial | Legal | Equality | Environmental |
| | No | Yes | No | No |

## 1. Introduction

1.1 Information Governance (iGov) is agreed upon ways in which the Council manages data and information. The three principal areas of interest at Stroud District Council are:

- **Data Protection** – The control of personal data. (GDPR etc.)
- **Government Transparency** – The proactive publication of information (Spending etc.)
- **Access to Information** - The reactive publication of information (FOI etc.)

1.2 In 2019 a suite of iGov policies and procedures was created to provide guidance for the key areas of this field. Since this time, and the last review in 2022, there have been best practice, technology, and risk changes which require that the existing documentation be reviewed again.

## 2. Overview of iGov work since 2022

- Creation of intranet support pages and guidance documentation covering all aspects of iGov.
- Improved data resilience and iGov knowledge across officers with training of ~50 champions and increased engagement across services to support individual needs.
- Developed accountability standards through improved reporting of iGov issues.
- In partnership with ICT improved the security of Council data using existing technology.
- Improved support for Subject Access and Freedom of Information request management.
  - We receive ~600 requests for information annually.
  - Yet we only receive an average of 6 information related complaints a year.
- Guided the introduction of responsible AI usage.
- Improved awareness of data related compliance across the Council.
- In partnership with the multiple services, developing new technology for improved complaints and information request management and reporting.
- Driven improvements to learning from data breaches by introducing the procedures in the Framework.

- Thanks to the work of our ICT team in securing and maintaining our infrastructure, we have very low occurrence of configuration and cyber related data breaches.
- Our key risk for data breaches, which is shared by most organisations, remains low risk 'human error' breaches, such as sending things to a wrong recipient or failing to redact information.
- As part of the breach procedure managers are providing learning actions to mitigate reoccurrence and officers are encouraged to take the time they need to get things right first time when managing sensitive and personal information.
- We have also developed clearer retention guidance and reiterated adherence to the data protection principles to reduce ongoing risks.

## 3. Review of the iGov Framework

3.1 To align with the Council values and improve accessibility for members and officers, the framework has been revised and consolidated in line with best practice from ~10 documents into a single, *One Council* reference and guidance document.

3.2 While iGov is informed by several pieces of legislation, individual decisions frequently rely on critical analysis of our framework by officers to reach the most suitable conclusion. This updated framework of one easy-to-use document will make the decision-making process easier and clearer when compared to using and cross-referencing multiple documents included in the previous framework.

3.3 If our iGov procedures fail for any reason this may cause negative consequences for our customers, potential monetary fines for the Council of up to £17.5 million per incident, possible claims for compensation and significant reputational damage. It is of note that in June 2022 the Information Commissioner scaled back the use of fines in the public sector noting: "In practice this will mean an increase in public reprimands and the use of my wider powers, including enforcement notices, with fines only issued in the most egregious cases."

3.4 The importance of having effective iGov policies and procedures is recognised and to reflect this there is a risk included in the Council's Strategic Risk Register on Ideagen which this committee reviews at each meeting. This risk (SR2) has appropriate levels of controls identified and the risk is regularly monitoring and reviewed.

3.5 We will continue to improve the accessibility and understanding of this often-complex area, with this revised framework being a key piece of the solution and mitigation if issues arise. We will ensure that the framework is continually updated with changes to legislation and best practice, and that any significant amendments will be brought back before this Committee.

## 4. Key Changes

4.1 Changed the following policy documents to procedures to reflect current best practice:

- Data Breach Policy
- Information Complaints Policy
- Anonymisation & Pseudonymisation Policy
- Records Management Policy

4.2. Reviews of the following policies:

- Surveillance Policy – Reduced size to focus on 'need to know' information
- Data Protection Policy – Amended to reflect current Council environment and best practice

4. 3 Added the following sections:

- iGov long term strategy – Aligned with the four Council values.
- Guidance on the use of artificial intelligence – To address member, officer, and public interest.
- Procurement guidance – To signpost importance of data protection in procurement.
- Information request procedure – To provide corporate approach to information requests.

## 5. Conclusion

5.1 Like many corporate functions of an organisation, you will seldom hear about iGov when it is working well. However, officers work hard every day to ensure we comply with relevant legislation, protect our customers data, deliver on our transparency requirements, and respond to the hundreds of information requests we receive every year.

5.2 The Framework confirms the Council's commitment to support the rights of individuals to request information and exercise other rights over their data. The Policy & Governance team will continue to support this work by making policy and process improvements to ensure that individuals can exercise those rights as easily as possible.

5.3 We also bring the Committees attention to the likelihood that major new data protection legislation is likely come into force within the next 2 years, the Data Protection and Digital Information Bill. When this legislation is enacted into law, the framework will be updated, and training provided to Officers and Members.

## 6. Implications

### 6.1 Financial Implications

There are no direct financial implications arising from this report. The cost of non compliance is significant and so it is important to have a framework in place.

Lucy Clothier, Accountancy Manager
Tel: 01453 754343 Email: lucy.clothier@stroud.gov.uk

### 6.2 Legal Implications

This report and iGov framework references the Council's statutory duties and obligations under the UK GDPR, Data protection Act 2018, FOIA and associated legislation and guidance. The Council has duties under this legislation in terms of accountability and compliance and must ensure it has appropriate policies and technical/organisational measures in place. The Council must also be able to show that it has adhered to the framework and associated policies, which may include awareness training, training, monitoring and audits.
A failure to ensure compliance could result in enforcement action by the ICO, damage to reputation and claims for compensation by aggrieved parties, amongst other things.

Iona Moseley, Lawyer, One Legal
Email: legalservices@onelegal.org.uk

### 6.3 Equality Implications

An Equality Impact Assessment has been completed but as there are no specific changes to service delivery proposed within this decision, no positive or negative impacts on any protected characteristics were identified.

The work undertaken to consolidate the Information Governance policies into one framework should improve accessibility as well as the quality and time of responses.

### 6.4 Environmental Implications

There are no significant implications within this category.

This page is intentionally left blank

STROUD DISTRICT COUNCIL
www.stroud.gov.uk

# Information Governance Framework

Strategy | Procedures
Policies | Resources

April 2024

Corporate Policy &
Governance

Stroud District Council
Ebley Mill
Stroud
GL5 4UB

Email: data.protection@stroud.gov.uk
Website: https://www.stroud.gov.uk/
Telephone: 01453 766321

# Contents

## Using this document

This document should be used as a reference manual. We recommend users search for a topic of interest by using the contents table or the search function of your software.

This public framework document evidences the Councils accountability and transparency when managing data lawfully and fairly.

The primary audience for this document is officers of Stroud District Council and references have been made to internal resources which assist officers to manage information enquires. To maintain the security of our systems and data, these proprietary resources will not be made public.

We will continually update this framework to reflect contemporary legislation and best practice. The document control section summarises the key changes made.

**Section 4.1 - Data Protection Policy, is mandatory reading for all employees and elected members of the Council.** This section may be presented seperately to this framework document as necessary.

# 1. Information Governance Framework

Information Governance (iGov) is the agreed management standards applied to all information used by an organisation. As a local authority, Stroud District Council processes substantial amounts of data across a range of services and requires comprehensive documentation to guide best practice. The key areas of iGov are:

- **Data Protection -** The control of personal data (e.g. GDPR)
- **Government Transparency -** The proactive publication of information (e.g. Spending)
- **Access to Information -** The reactive publication of information (e.g. FOI)

This framework document collects the topics of iGov together to support Council stakeholders to make informed decisions. Each section can be referenced in isolation or in combination with other topics.

All employees, elected members, contractors, consultants, and other stakeholders involved in the collection and processing of data for, or on behalf of, the Council have a responsibility to ensure they are complying with data legislation and Council procedure.

The key pieces of legislation iGov relies on have been listed in the legislation section. Individual Council services also have specific regulations they need to comply with, and services must understand how their own requirements interact with the legislation in this document.

Information Governance is an evolving discipline and to ensure stakeholders have the support they need this framework is reinforced by a range of internal documentation, training, and specialist support from the Information Governance Officer, Data Protection Officer, and the Council legal services provider, One Legal.

# 2. Information Governance Strategy

The long-term strategy for iGov is explained using the four values of Stroud District Council:

**Valuing Our People**

Officers and Councillors will be supported to confidently manage Council data in a fair, lawful and transparent manner. They will be provided with all necessary training and guidance to support this purpose, and resources will be regularly reviewed to comply with contemporary best practice, legal requirements, and Council goals.

Support and development will be tailored to meet the specific needs of services with additional focus given to the officers responsible for administrating and responding to information requests and data protection enquires.

**Making a difference**

There are two main uses of data in the Council, the primary being the delivery of services and the secondary being the analysis and improvement of these services.

iGov will make a difference through the continual review of processes, driving a data by design approach by encouraging consideration of data protection and innovation from the earliest opportunities, and by continually seeking of feedback from stakeholders and communities to ensure data use is relevant and of value.

Corporate data will be used for business intelligence, strategic development, research, compliance, and transparency purposes. Where appropriate, system and process improvements will be suggested when they will provide a tangible benefit to the organisation.

Failures of compliance will be managed through rectification and enforcement measures as appropriate.

**Aiming High**

iGov will support transformational programmes and Council Plans by providing guidance and resources as appropriate. Where there is clear added value to the organisation or our communities, iGov will recommend performance, technology, and process improvements.

**One Council**

All stakeholders of the Council will be supported to deliver their data obligations, and opportunities will be identified to connect services and projects together where similar data is being used. iGov will be accessible to all officers and Councillors and drive a joined-up, modern approach to data management.

iGov will not be a barrier to the completion of Council work or transformation, but a useful tool to ensure the appropriate use of data throughout the Council, and a guide for continual improvement of data use.

## 3. Roles & Responsibilities

- **Data Protection Officer (DPO)** – A statutory role required of a local authority. Fulfilled at Stroud by the Monitoring Officer as a joint role. The DPO oversees the organisations compliance, informs and advises on data protection obligations, provides advice, and acts as a contact point for data subjects and the Information Commissioner's Office (ICO). May manage and respond to information complaints. SDC is registered with the ICO under reference: Z6903475.
- **Senior Information Risk Owner (SIRO)** – Fulfilled by the DPO. The SIRO provides executive level accountability for information risks.
- **Electoral Registration Officer and Returning Officer –** Fulfilled by the Chief Executive of the Council. A separate controller with the ICO, responsible for the data protection of all elections managed by the Council. The ERO is registered with the ICO under reference: ZA146754.
- **iGov Officer** – Operational management of iGov functions and the main support contact for the organisation. Deputises for the DPO. Responsible for developing the iGov framework, procedures, accountability, resources, and training. May manage and respond to information complaints.
- **iGov Champions** – Council officers with additional responsibilities to manage and administrate information and data protection requests. Approximately 50 officers support these functions.
- **Information Asset Owners** – Usually heads of service or senior managers. These are the individuals with overall responsibility for the flow of information through their service and the enforcement of any legal/regulatory requirements.
- **Head of Technology**- iGov works closely with the ICT service as the management of data usually involves an element of technology or digital control. Management of the technical implementation of security, software and hardware within the Council is the responsibility of the Head of Technology.
- **Management Officers** – In the context of information governance, management may be responsible for an asset, system, area, or record(s). They are responsible for ensuring compliance with all applicable policies and procedures in their management area and ensuring colleagues and stakeholders understand their responsibilities.

- **Council Officers –** Employees of the Council. All officers of the Council have a responsibility to use Council data lawfully. Officers must understand the data protection policy and any other sections of this framework relevant to their work. Any queries related to data should be raised with the iGov officer promptly so appropriate support can be provided.
- **Elected Members (Councillors) –** Councillors are elected by their constituents to represent public interests at the District Council. Councillors will perform work for their constituents and as a district representative. They are generally controllers of ward and constituent data and processors of District Council data. Councillors do not have a right to access Council data beyond that which is required to fulfil a lawful purpose or in support of a constituent. Councillors must advise officers of the capacity in which they seek data, e.g. as a private citizen, a district Councillor or in a support capacity for a constituent. Councillors are not required to register with and pay a fee to the ICO as data controllers, but they must comply with the data protection legislation.
- **Other Stakeholders –** Other stakeholders such as customers, contractors, and consultants should also only use data in a fair and lawful manner. Any identification or suspicion of Council data being used improperly should be reported to the Council immediately.

# 4. Policies

## 4.1. Data Protection Policy

As a local authority we provide services to over 120,000 residents and many businesses, tourists, and community groups. To deliver these services it is vital that we collect and use information about our customers, staff, suppliers, and other stakeholders.

All Council officers, Councillors, and others working on behalf of Stroud District Council have a responsibility to use data lawfully and respectfully. Additionally, individuals have rights they can exercise over their own personal data which everyone in the Council must be aware of to identify and respond appropriately.

This policy may be updated at any time to reflect current best practice and legal requirements. For any concerns about data protection please contact the Data Protection Officer, Information Governance Officer, or email data.protection@stroud.gov.uk. Always ask for support if you are in any doubt about data management. Failure to adhere to this guidance and the information governance procedures may result in disciplinary action.

**What is data protection?**

Data protection is the control of personal data. Personal data is any information that can be directly or indirectly used to identify a living individual. It can be in any format and common personal data includes names, images, and health information. Personal data can also include less obvious information such as opinions and behaviours related to individuals.

All personal data we process is subject to legal safeguards defined in the Data Protection Act 2018 and the associated UK GDPR 2021. For definitions and legislation please see the relevant sections of this framework.

While this policy specifically relates to personal data, the principles are applicable to all data and provide a solid foundation of responsible information governance.

**Why is it important?**

We know that our customers and colleagues value their privacy and rightly expect us to manage their information respectfully and lawfully. The way we can evidence that we are doing this, and be accountable for our actions, is to comply with data protection law and best practice.

If an organisation gets data protection wrong, there can be significant consequences. As a local authority we can be fined up to £17.5 million by the information commissioner, suffer significant reputational damage, and potentially be unable to deliver our services.

The misuse of data can also cause real harm to individuals. We call the misuse of personal information a data breach as the expectations of how the data should have been used has been broken. Examples of data breaches include accidentally sending personal information to the wrong person or losing an insecure device. Serious data breaches may lead to fraud, identity theft, violence, or exploitation if personal data is mishandled. If you ever suspect a data breach has occurred, immediately follow the data breach procedure.

A confident and applied understanding of data protection is vital for anyone involved in the processing of personal data.

**Responsibilities as a representative of the Council**

One of the ways we evidence our data protection competence is with training. All officers and Councillors must complete annual data protection refresher training to demonstrate their ongoing understanding of the topic. Officers and Councillors will receive annual reminders which must be completed. Failure to complete training may result in disciplinary actions or account suspension to protect Council assets and personal data.

Should officers and Councillors have any queries or concerns about data protection they are encouraged to consult this framework, check the intranet (search: iGov), or contact the iGov officer or Data Protection Officer for support.

Anyone working with Council data must ensure they are familiar with the following data protection principles. These provide a strong foundation of understanding that can then be enhanced with specialist role knowledge. Our regulator the ICO has further detail on each of these principles:

- **You must ensure data is processed lawfully, fairly, and transparently.**
    - We need to make sure that anytime we are processing personal data we understand why we are doing it, that we have a lawful reason to do it, and that we are fair and transparent with the people whose data we are using.
    - Most of what we do at the Council is required by law as a public authority or as a contractual obligation. We explain our reasons for using personal data via our privacy notices on stroud.gov.uk/privacynotice. Occasionally a hardcopy privacy notice or terms may be provided. If we receive data from someone else, such as a referral, then the originating organisation should ensure the customer knows how their data will be used.
    - There are six main lawful bases for processing personal data. For existing Council work these are already defined and explained in our privacy notices. It is only when you want to make a significant change or start something new that you will need to choose the basis for the processing. Officers and Councillors must contact iGov before they start new personal data processing, to ensure customers are adequately informed. Please see the ‘starting new data processing’ section for more detail.

  - The lawful bases are:
    - Public Task (providing statutory services)
    - Contractual Obligation (e.g. a tenancy agreement)
    - Legal Obligation (e.g. safeguarding)
    - Consent (when someone gives us permission)
    - Legitimate Interest (where we make a judgment to process)
    - Vital Interest (life threatening situations)

- **We only process data for specific purposes.**
  - Anyone processing personal data should ensure it is only used for the purposes we have set out in our privacy notices or other signposting to the intended customer or data subject.
  - Where we need to use personal data for another purpose, we must have a clear lawful basis for the new processing. We will not do any additional processing incompatible with the original purpose without a new basis.
  - No stakeholder of the Council shall use personal data for a purpose not authorised by the Council or explicitly agreed to by a data subject. To do so may be investigated as a disciplinary action or a breach of contract and could be a criminal offence.

- **We only process the minimum data required to achieve that purpose.**
  - We do not collect data 'just in case'. We only collect the data we need to fulfil our specific purposes.
  - Where we are using data for a secondary purpose, such as analysis, we will use techniques such as anonymisation where appropriate.

- **We ensure data is accurate at all times.**
  - We will always action genuine updates and corrections to data.
  - We will replace or destroy inaccurate data promptly.

- **We only store data for as long as is necessary for these purposes.**
  - We will not keep personal data 'just in case'. Once data has fulfilled its use, we will deal with it appropriately.
    - This usually means destroying data, but it can also mean anonymising, redacting, or archiving as required.
  - The Council has a retention schedule which lists all the key records processed, how long they will be kept, and what happens to them after this period. The most up to date version can be found at stroud.gov.uk/privacynotice. Services are responsible for ensuring their records are included in this schedule by informing the iGov officer.

- **We ensure that data is stored securely and confidentially as appropriate.**
  - The Council uses secure passwords and two-factor authentication to control access to Council data. Officers must familiarise themselves with the Councils Information Security policy which can be found on the intranet.

    - No one with access to Council data will extract it to devices not owned or controlled by the Council without permission from ICT or the DPO, and a specific legitimate purpose.
    - Those with access to Council data will never access information without a lawful basis.
    - Data will only be shared with people who 'need to know' and only for a specific purpose. Any sharing must follow the data sharing procedure.

- **We are accountable for the data we process by**
    - Reporting any data issues to our manager, the iGov officer or the DPO.
    - Reporting if security or access credentials have been lost or compromised.
    - Reporting any data breaches or incidents immediately to our manager and the iGov officer.
    - Declaring any potential conflicts of interest related to data access as part of an annual employee declaration.
    - Maintaining accurate records and registers related to effective information governance.

### Considerations

1. This framework should be referred to for any processing someone is unfamiliar with or that they have not completed in some time. The various procedures included in this framework should be consistently applied across the organisation. Additional practical information is available on the intranet.

2. All Officers and Councillors must assist the iGov champions as requested to fulfil Freedom of Information (FOI) and other data requests. We have legal requirements to complete most information requests within 20 working days and GDPR Individual rights requests, such as Subject Access Requests (SAR), within one calendar month.

3. Processing children's personal information – Children have the same data rights as adults. The Council position is that, in general, a child aged 13 or over can make decisions related to their own personal data. Children aged under 13 or who are unable to confidently understand their rights can be represented by a responsible adult. The responsible adult must provide evidence of ID and/or their relationship to the child to receive data and the Council reserves the right to withhold information where there is any suspicion of data misuse. Age 13 is chosen as this is the age individuals in the UK can legally provide data related consent under the Data Protection Act 2018.

4. Exercising of **individual rights** – Individual rights are granted under the GDPR. They guarantee us the ability to access our own data and correct it when it is wrong. There are also situational rights that can, in certain circumstances, allow us to delete our data or stop it being processed. Officers and members should understand when an individual rights request is being made so we can ensure we are managing them effectively. The above link will provide an overview of the rights and the procedure to fulfil them.

5. **Special category data**, which is sensitive data with extra controls such as information related to health or ethnic origin, requires a separate lawful basis to other data processing. For any new processes involving special category data, the information or process owner must contact iGov to assess the processing and assign the appropriate lawful basis if the use is required. The special categories of data have all been used to persecute groups of people which is why they require additional safeguards.

6. When services want to create a new process, buy/use a new system, or any other new activities that involve personal information; they must contact the iGov officer to consider a Data Protection Impact Assessment (DPIA) before any procurement or usage. This assessment is essentially a recorded checklist to ensure that we have met all the data protection principles, have mitigated the risks, and really thought about how data will be used. A DPIA is mandatory for any potentially high-risk processing, such as using CCTV.

If you are ever in any doubt about the use of personal data, cease all processing and contact iGov.

## 4.2. Surveillance, Covert Human Intelligence Sources, and Acquisition of Communications Data Policies

### Overview

There is a difference between general observations and surveillance. Information gained as part of routine patrols of communities such as in the case of neighbourhood wardens and housing officers going about their duties, and officers passing an area and observing an incident are general in nature and not surveillance.

The use of CCTV for general monitoring and safeguarding of the public is not surveillance for the purpose of these policies. Many of the public street cameras owned by the Council are managed by Gloucestershire Constabulary for the ongoing prevention and detection of crime.

The key contacts at Stroud District Council for surveillance enquires and complaints are the RIPA Coordinator in the Counter Fraud and Enforcement Unit (emma.cathcart@cotswold.gov.uk) and the Data Protection Officer (data.protection@stroud.gov.uk).

The policies governing this area and adopted by the Council are:

- Regulation of Investigatory Powers Act 2000 (Surveillance and Covert Human Intelligence Source) Policy
- Investigatory Powers Act 2016 Acquisition of Communications Data Policy
- Use of the Internet and Social Media in Investigations and Enforcement Policy

These must be adhered to and set out practical guidance for the use of surveillance by and on behalf of Stroud District Council. Surveillance will only be used to achieve a clear and specific aim, and in accordance with these policies.

For key definitions, legislation, and practical processing officers should refer to the Biometrics and Surveillance Camera Commissioners code of practice (November 2021).

## Regulation of Investigatory Powers Act 2000 (RIPA)

RIPA is designed to protect an individuals' Human Rights from interference from public bodies and prevent Councils obtaining personal and sensitive personal data about individuals without justification. They instead must show that they are investigating a crime, and the actions are necessary and reasonable in order to achieve a defined objective.

If Councils do not adhere to the legislation or internal policy and undertake activities that are deemed to breach a person's Human Rights then the Council could be heavily financially penalised.

- Councils can undertake surveillance if it is not intrusive, and they consider necessity and proportionality.
    - Necessity - the aims and objectives, what other options have been considered and why surveillance is now appropriate.
    - Proportionality –the scope, and duration, the seriousness of the offence weighed against the anticipated results.
- Surveillance can be physical monitoring – following, photographing, observing, listening – or less obvious monitoring such as via social media.
- Councils cannot carry out intrusive surveillance – such as hidden cameras inside someone's home or phone taps.
- Serious Crime Threshold – if the crime is a more minor crime Council's cannot use RIPA, however as good practice, the Council's policy states that the officers must still complete a similar non-RIPA application to obtain authorisation for any surveillance activities.
- If the offence meets the threshold the application goes to a Magistrate for authorisation. If it is a non-RIPA application it is authorised by one of the Authorising Officers within the Council.
- The application must consider all the risks associated with the surveillance operation including the risk of collateral intrusion (obtaining sensitive personal data about unconnected individuals) and how this will be mitigated. It must also give full details of the crime being investigated, the reason it is felt appropriate to undertake surveillance, the aims and objectives, what other investigation methods have been considered/utilised already and how any risks will be mitigated.
- RIPA only applies to public bodies (not individuals/private organisations) however, Council officers cannot instruct others to undertake surveillance on their behalf or use intelligence/evidence gathered by an individual conducting covert surveillance.

## Investigatory Powers Act 2016 (IPA)

This Act gave Councils additional powers to obtain communications data when investigating criminal offences.

As with surveillance the IPA seeks to protect Human Rights and prevent public bodies obtaining personal data without considering whether it is proportionate and justifiable.

- Councils can obtain 'entity' data – such as the subscriber for a mobile phone number, or whom a handset or email address belongs to - in relation to criminal investigations. This can be obtained from any communication provider in the UK, including postal communication companies.
- If the offence meets the Serious Crime threshold then Councils may also be able to obtain 'event' data – such as where a device was located when calls were made, when data was downloaded or itemised phone bills showing what numbers have been called and the duration of the call.

- All Council IPA requests must go through a single point of contact (SPOC) – National Anti-Fraud Network (NAFN) – who check and verify the application before it is authorised by the Office for Communications Data Authority (OCDA).
- The Council has a Designated Person (the RIPA Coordinator) who is notified when any IPA application is made to ensure the Council is aware of the request.
- The NAFN SPOC must ensure that the application demonstrates necessity and proportionality and how risks of collateral intrusion will be mitigated and dealt with before they send for Authorisation.

## Use of Internet and social media for investigation and enforcement

Using social media and the internet to obtain intelligence and evidence could stray into the realms of surveillance, and therefore the Counter Fraud and Enforcement Unit has introduced a policy relating to its use.

This sets out some of the risks, and the appropriate safeguards, associated with Councils using open-source material in investigations. Officers can access this and the other specific surveillance policies on the Council intranet.

## Camera Locations and System Management

Overt cameras / CCTV for general monitoring may be installed:

- In Council owned buildings such as Ebley Mill, Council-owned leisure centres and the Museum in the Park.
- In Communal areas of Council owned housing, such as hallways in blocks of flats, courtyards, and independent living schemes.
- In Council owned vehicles.
- On individual officers in the form of body-worn cameras.
- Permanently in public areas of the district such as town centres and parks with facilities. These cameras are owned by Stroud District Council but operated by Gloucestershire Constabulary and are governed by the constabulary code of practice.

Overt or covert surveillance cameras may be installed:

- Temporarily in public areas of interest for directed enforcement activities such as monitoring fly-tipping hotspots.

For overt surveillance, signage will be present at the entrances of buildings, sites, or near to the area of camera operation.

Whenever a new site, purpose, or installation of a CCTV or surveillance system is proposed a Data Protection Impact Assessment (DPIA) must be completed prior to any installation. These assessments determine whether the system is the most appropriate solution and if so, justifies its use through evidenced compliance with data protection legislation and the surveillance code of practice. Separate to the DPIA an operational assessment will be completed by the relevant Council service to ascertain the most appropriate system to use for the required purpose.

Footage from cameras is continually recorded, unless motion or user activated, and overwritten as storage devices fill up. Camera data is only exported where an investigation needs to take place. The Council may use footage to investigate allegations of crime, fraud, for internal disciplinary purposes, or to fulfil individual rights requests under the data protection act.

Audio is not recorded by default unless using a body-worn camera. Audio can only be recorded where this is deemed a necessary measure to fulfil a surveillance purpose and it is recorded in the system assessment and DPIA. Data recorded by Council operated surveillance systems remains in the ownership of Stroud District Council.

The Council maintains an inventory of camera locations, assets installed, approximate retention periods, servicing logs, image quality ratings, and responsible officers. Systems are only accessible by select officers who ensure the security and integrity of the systems they manage.

Covert surveillance, by its nature, could be deployed anywhere an investigation is required. Any activity of this type must be documented and authorised by the Counter Fraud and Enforcement Unit and nominated senior officers and is reported annually to Audit and Standards Committee. All covert surveillance must also have a DPIA completed.

All surveillance systems will be maintained by the service they relate to, aiming for maximum uptime and compliance with the objectives of the installation. Specialist surveillance contractors shall be used as appropriate with collective One Council contracts encouraged over separate procurement for each service.

### Sharing and disclosure of surveillance data

Surveillance data is managed in accordance with data protection legislation and the surveillance code of conduct. Any requests for the sharing or disclosure of surveillance data must be managed by the iGov officer to maintain a consistent approach and an accurate record of disclosure.

Data will never be shared more widely that is necessary for a specific purpose, and only with those who ‘need-to-know'.

Routine reasons to share surveillance data include:

- Providing evidence to the Police or other statutory body. These requests must be supported by a formal written request form, citing the specific legislation and reasons for disclosure.
- To the public or their representatives under a subject access request or other legitimate reason such as for insurance investigations, or for the due process of a legal claim. Any such requests must give details of location, time, and event to support the request. Requests made to the Council for data held by Gloucester Constabulary (e.g. street cameras), will be directed to contact the Police. Data will not be shared when it relates to an ongoing criminal or enforcement investigation to avoid prejudicing due process.

Council officers will consider what collateral data may be disclosed when sharing, such as the personal information of others, and use applicable redaction techniques as appropriate.

This policy will be kept up to date to reflect changes to legislation, code of practice and best practice. Officers managing surveillance should be familiar with the rest of this framework as the topics are closely interconnected.

## 5. Procedures

### 5.1. Data Anonymisation

Anonymisation should be used where there is a legitimate reason to process information for a secondary purpose, but it is not appropriate to use the personal or sensitive parts of it. Common examples include for research and development, statistics, transparency data, archiving, and information requests.

For the purposes of this procedure, we will use the word anonymisation by default. Officers should understand the differences between this and pseudonymisation and pick the most appropriate method for their needs. The different methods are described in this procedure.

The ICO has an anonymisation code of practice which supports decision making and includes detailed information on specific scenarios. Officers can also contact the Information Governance Officer or Data Protection Officer for advice.

Anonymisation helps to protect the privacy of individuals while balancing the need for government transparency and informed research and development. The Data Protection Act requires us to protect personal information from inappropriate use and disclosure, and anonymisation is a very useful tool to ensure we meet this requirement.

Any individuals processing data for or on behalf of the Council should be aware of the proper use of anonymisation. This procedure may not apply where there is a specific information sharing agreement or other mechanism in place to share data externally in a lawful and secure manner.

Anonymisation should not be a substitute for the destruction of data where it is no longer necessary for a purpose. Personal Data should not be kept 'just in case,' but only where there is a legitimate reason for its retention.

## When to anonymise

When considering if anonymisation is required it is useful to assess the situation against the following criteria:

a) If a decision is being made about an individual or to provide services to them, it is usually a requirement to be able to identify them using personal data. In this situation it is unlikely that the data should be anonymised.

b) If the data is needed to analyse or plan on a larger scale affecting a service, population, area, or is being made public, anonymisation may be required.

**Ask yourself: Do I need to know who individuals are to be able to make the decision?**

Before anonymising data, you should also consider:

**The risk of re-identification –** Before you publish any data, think about whether it is likely that there exists other accessible information that could be combined with your data to re-identify individuals. The risk of reidentification is highest where data contains only a small number of subjects or is unique in nature, it is less likely in large or routine data sets.

In practice this means if you wanted to identify the individuals, can you reasonably do so with existing information and could you put in additional security or dummy data to remove the risk?

**Assessing the purpose –** Even if someone is requesting anonymous data, we must still assess whether the purpose for processing it is valid. Think about:

a) Does the anonymous data risk any commercial interests or could it prejudice the effective creation of policies and plans?
b) Does the person requesting the data have a 'need to know'? If not, you should challenge the request and signpost to any more appropriate data already available.
c) If the request has been made via Freedom of Information or Environmental Information Regulations, it is effectively being given to the world at large. Could that have any consequences?

**Examples:**

1) A member of the public has requested the number and type of planning enforcement actions for the last year, broken down to parish level under an FOI request.

In this instance anonymisation is suitable. The public do not need to know any personal information for the purpose to be served. Therefore, the data is anonymised via generalisation to only the parish level and any personal identifiers removed. An individual anonymised enforcement action may simply read: “Stonehouse – breach of conditions”

2) A manager requests the whole organisations HR data showing absence reasons and periods over the last year. They want this to understand how their service compares to others and assess how they can reduce absence in their own service.

Although it is internal, it would not be appropriate to provide the manager with the personal information of all individuals who have been absent. However, there is a benefit to understanding how their own service fits into the bigger picture of the organisation. Therefore, HR could provide anonymised statistics showing absence reasons for the whole organisation.

### How to anonymise

1) Select your anonymisation methods:

Depending on what data you need to process, you may need to apply more than one of these methods.

a) **Anonymise -** If the data is being provided as a one off or will be published to the world at large (i.e. responding to an information request or being published on a website) full anonymisation is usually recommended. This is the ***removal or replacement with unidentifiable data*** of all personal information from a data set.

| Original Name | Anonymise | Anonymised Name |
|---|---|---|
| Naomi Nagata | > | redacted or deleted |
| James Holden | > | redacted or deleted |

b) **Pseudonymise -** If the data is being used as part of a wider project or for research and development you may wish to continue to be able to identify individual datasets throughout the project and across documents, but without the direct identification a name or account number would cause. In this instance you will use pseudonymisation to ***consistently substitute*** the personal information.

| Original Name | Pseudonymise | Pseudonymised ID |
|---|---|---|
| Naomi Nagata | > | 23PJN01 |
| James Holden | > | 23PJN02 |

c) **Generalise/Aggregate -** If you require a level of detail to be able to serve your purpose, but full personal information is not required you can generalise data to make identification more difficult. This is very useful for statistical data such as survey results, census outcomes and information requests. You can also aggregate by consistently manipulating an integer across every field but not disclosing the exact adjustment to reduce re-identification risk. E.g. multiply each field by 0.6 or add 12.

| Date of Birth | Generalise | Age Range (as of 2023) |
|---|---|---|
| 05.08.1976 | > | 40-50 |
| 18.04.2001 | > | 20-30 |

Whichever approaches you take you must assess each field of personal information for purpose and apply your chosen approach to the data you do require.

**Remember:** This is real people's data; we are trusted to protect their privacy rights and use it only for lawful purposes. Data should only be accessed by those who need to know, and we should use the minimum required to fulfil our purpose.

It is recommended that prior to the publication of any anonymised data, a second opinion is sought to check for any likely issues. You can also contact the iGov officer or DPO if you have any questions. For specific systems and methods of how to redact, search 'redaction' on the intranet.

### 5.2. Data Breaches

A data breach is where personal data is accidentally or unlawfully destroyed, lost, altered, disclosed, accessed, transmitted, stored, or otherwise processed. It is a broad definition and breaches can occur for many reasons but chiefly due to:

- Inadequate system configuration (e.g. firewall rules or excessive permissions).
- Cyber-attack and Malware (e.g. phishing or hacking attacks).
- User error (e.g. wrong recipient, weak passwords, or loss of data).

Personal data breaches can have varied impacts ranging from mild inconvenience through to danger to life. As a Council we are pro-active in the reporting of breaches as we understand that they affect people and are an opportunity to learn and improve. Where breaches do occur, the following procedure will apply. Officers also have access to documentation, reporting forms and practical guidance on the intranet (search: data breach).

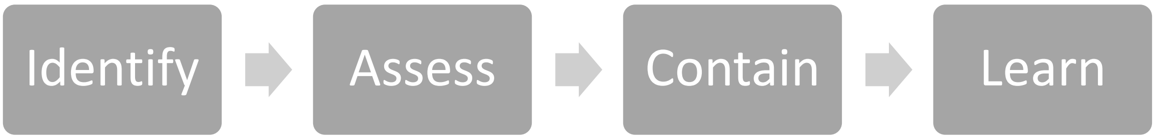
To minimize the risks of a breach all employees and Councillors of the Council must ensure they are familiar with the Information Security policy owned by the ICT team, the Data Protection policy, and complete their annual refresher training.

All stakeholders involved in Council matters must take responsibility for ensuring the data they process is done so fairly, securely and with due care and attention to minimise the risk of a breach. Anyone identifying or being told about a breach must report it to their line manager and the iGov Officer or DPO as soon as possible.

Contractors, Consultants, Suppliers, and other entities acting as a controller or processor must inform the council of any data breaches involving or suspected to involve Council data. The Council will do likewise with any third-party data involved in a breach. All contracts must have data protection clauses that include data breach responsibilities.

All breaches and incidents are recorded on a breach register held securely by the iGov Officer. This register aids learning and monitoring at a corporate level as well as being a reference for our regulator the ICO.

When a suspected breach is reported the relevant service area should follow the steps outlined below. Officers will not admit fault or contact data subjects without express permission of the DPO. Upon discovery, it is important to only gather information and confirm that we will investigate. Premature actions and conclusions can lead to additional harm or exacerbate a breach. The following steps will be taken to manage a personal data breach:



### Identify

A suspected breach can be identified by anyone. As soon as the Council receives information about a breach the receiving person must ask questions to identify the scope of the breach and understand the incident. The Council has a breach reporting form to assist in gathering this information, available on the intranet (search: data breach).

- What is the suspected breach, what happened?
- What data is involved in the breach?

### Assess

Next the receiving person should ask the following questions to gather preliminary information about the cause and understand the likely consequences.

- How did it happen?
- When did it occur?
- Who and how many people does it affect?
- How far has the data spread?
- What are the likely effects?
  (This is usually a snap judgement, and we do not expect receiving officers to fully assess the impact at the initial point of contact)

The receiving officer will then send the completed form to the iGov officer and/or DPO where a full assessment will be completed using established criteria recommended by the ICO. We will assign a severity level of low, medium, or high. In general, a breach becomes more severe the less secure the data is, the more people it affects and the more sensitive the data included. For example, a name and address in isolation is generally low risk. Whereas a name and address in the context of an at-risk individual could be high risk. Every assessment is unique, and we will always consider individual circumstances.

Low and medium severity breaches may cause some temporary inconvenience to individuals or issues which might impact service delivery. Officers may take appropriate actions immediately to minimise the impact of these levels of severity.

A high-risk breach is likely to “lead to physical, material or non-material damage for the individuals whose data have been breached” and must be reported to the ICO within 72 hours of us being made aware of it. In the event of a high-risk breach the DPO will make any decisions about informing the ICO and data subjects. Officers must not take any actions on a high-risk breach without authorisation from the DPO.

### Contain

Once assessed, if the breach is a low or medium risk the receiving officer should consider what actions they can take to contain the breach safely at the earliest opportunity. If assessed as high risk, no actions are to be taken without the authorisation of the DPO.

- Can we do anything immediate to stop the data spreading without additional risks?

- Can we retrieve or destroy the data?

This can often be as simple as emailing the recipient of the data to ask them to delete it or removing it from a website. Depending on the number of recipients or nature of the breach there may not be any accessible or appropriate actions to take. If the officer has any concerns, they should take no action and instead contact the iGov officer and/or DPO.

The actions required to resolve a breach are varied and will depend on the circumstances and severity. In general, resolving a breach may involve degrees of securing data, destroying data, monitoring activities, consulting with involved parties, amending or improving security measures.

#### Learn

Once a breach has been contained and resolved as far as possible, the originating service, with support from the iGov Officer, will record the learning outcomes to mitigate further risks. It is the responsibility of service leadership to implement mitigation actions. Repeated breaches with the same root cause will be escalated to the strategic leadership team.

All breaches related to services will be fed back to the head of the relevant service for transparency and accountability. Breach statistics are also assessed by the Corporate Governance Group.

- How can we prevent the breach reoccurring?
- What measures could we take to minimise the ongoing risks?
- Are there lessons that can be applied to the whole Council?

The details of breaches including learning outcomes are recorded and monitored securely by the iGov officer. One year after a breach is resolved, register data will be anonymised.

### 5.3. Starting new personal data processing (new systems, processes etc.)

Where a service or individual wishes to start a new type of personal data processing, they must ensure **before** any processing takes place that they have:

- Assessed the proposal against the data protection principles,
- Considered whether the proposal involves a new type of processing to the Council or involves any high-risk processing; and if so have completed a data protection impact assessment to evidence compliance.
- Considered that if data is being shared with external parties routinely, is there a contract and/or sharing agreement in place? (we cannot process data routinely without these).
- Recorded the information required for a privacy notice and sent this to iGov for review:
  - Why do you need to process the data (reason and lawful basis)?
  - What personal information are you processing?
  - How will it be collected?
  - Who will you be sharing it with (external only), is it shared outside of the UK or EU?
  - How will it be secured and accessed (is access restricted to a group etc.)?
  - How long will the data be retained and what is the basis for this (a specific law etc.)?

If your process requires the use of special category data, there are additional safeguards required. We will need to:

- Select the appropriate lawful basis from Article 9 of the GDPR
- Where applicable, select the appropriate paragraphs for reference from schedule 1 of the DPA 2018 to support the need to process this data

These checks should be completed prior to any new procurement or collection of data. If in doubt, please contact iGov to discuss your requirements.

## 5.4. Data Sharing

Data sharing is vital to the delivery of Council services and falls into two broad categories, ad-hoc and routine. This procedure only applies to the sharing of data with external parties. The movement of data internally, while not data sharing, is still subject to the data protection principles and good record management.

No sharing can take place without a valid lawful basis. The sharing of personal data must be transparent to those whose data is being shared, usually by inclusion in the Council privacy notices. For one off events and smaller projects separate signposting can be provided to data subjects.

The ICO has a data sharing code of practice which is used as the reference for Council data sharing. Officers also have access to a data sharing agreement template and other practical guidance on the intranet (search: data sharing).

Data Sharing is situationally dependent, and each service is responsible for ensuring that they seek out any advice needed when proposing to share data to deliver a service or project.

The Council is a participant in the Gloucestershire Information Sharing Partnership Agreement (GISPA) which is a set of principles governing minimum standards when sharing data across county partners. This agreement has its own sharing template for partners to use.

### Ad-hoc Requests

These are usually one-off requests or only required to fulfil a single purpose. Common examples include requests from Police for missing persons, proof of life, or apprehension of criminals; and government departments such as HMRC and the Department of Work and Pensions for counter-fraud works.

Ad-hoc requests must be supported by legislation usually found in Schedule 2 of the Data Protection Act 2018. This legislation explains when sharing can be exempted from the GDPR.

Sharing will not take place without a specific legitimate purpose being evidenced by the requestor and the request being satisfied as non-fraudulent by council officers. To ensure consistency and accountability, all requests of this nature received by services must be forwarded to the iGov Officer before any information is provided. Ad-hoc requests will be centrally managed and recorded on a register, which is anonymised after one year.

### Routine Requests

Routine sharing makes up the bulk of the data shared by the Council as it is usually required for service delivery, a long-term project, or other structured agreement.

Routine sharing rules and limits must be agreed prior to any sharing happening. As with all sharing, there must be a clear purpose and lawful basis to share information.

Sharing terms must be set out in a contract or specific sharing agreement and clearly explain the reasons why sharing is required, what will be shared and with whom, who is responsible for the data and when, and any security and communication requirements in case of a data breach or other data security issue.

The ICO have a data sharing checklist which is a useful reference for this purpose. The Council also has a template sharing agreement available on the intranet.

If a project or service has got to the stage where sharing is required, it is reasonable to assume that the project lead will understand the full scope of sharing requirements. Sharing where there is limited understanding of what is needed and why is a sign of an incomplete project plan and should be addressed before any sharing commences.

The iGov officer can assist officers to create suitable sharing agreements.

### Data Protection Impact Assessments (DPIA)

A data protection impact assessment must be completed where there is any high-risk personal data processing, where a contract, project or programme is a major works, or when sensitive data is being shared. It is important that the DPIA is completed before any sharing begins.

The assessments are risk management checklists that support project leads to think about:

- What risks does this process/sharing have related to data?
- What are the alternatives to processing/sharing?
- What controls and actions can be put in place to mitigate the risks?
- How will we monitor any ongoing risks?

While DPIA's are only mandatory for high-risk processing, we encourage officers to use them for other projects and services to evidence data protection accountability.

Officers should contact the iGov officer to discuss whether a DPIA is appropriate for their project. The completed assessment will be stored by the relevant service and the iGov officer. More information is available on the intranet (Search: DPIA).

### Data Sharing, Transparency, and Information Requests

As a public authority, we have significant transparency requirements, and it is important to be clear with third parties, such as project partners and suppliers, that any data they share with the Council may be disclosable under transparency rules.

Commonly this means disclosure under an FOI request or as part of a committee or Council paper. We encourage consultation with third parties if their data may be disclosed, and officers should apply appropriate exemptions to protect individuals and commercial interests; however ultimately it is our decision as the public authority whether we disclose information or not.

## 5.5. Individual Rights Requests

Under the UK GDPR, individuals may have certain rights they can request we perform with their personal data. Officers should be familiar with these rights and understand how they interact with our service delivery. The ICO provides a primer on each of these rights on their website. The rights and when they apply are:

- The right of access [Always]
- The right to rectification [Always]
- The right to be informed [Situational]
- The right to erasure [Situational]
- Right to restrict processing [Situational]
- Right to data portability [Situational]
- Right to object [Situational]
- Rights related to automated decision making [Situational]

For rights requests outside of our normal service delivery, the iGov officer will record them on a secure register for monitoring purposes.

As per the data protection policy, in general any person capable of understanding their rights and who is at least 13 years old may exercise them.

To exercise a right, the Council must be satisfied that the person making a request is the data subject. Depending on the situation identity may be confirmed by passing phone security checks, providing valid ID, or other appropriate method an officer chooses.

Individuals can ask third parties to make a request on their behalf such as a solicitor, friend, or family member; however, identity verification and explicit consent from the subject to authorise the third party are required to fulfil a request.

### Right of access (SAR)

This is commonly known as a subject access request. Individuals always have this right. A person may request their own personal data held by an organisation. A SAR can be specific or general. A specific request is always recommended as it allows the limited resources of the Council to focus on an in-depth search. A general request such as ‘everything’, will receive a general response as the resources will be spread more thinly.

A request for personal information usually becomes a SAR if it is asking for data above and beyond what we would provide as part of our normal service delivery. The Council has one calendar month to provide the personal information we hold. We will query any requests which are unclear or do not meet the criteria of a SAR.

The right of access only applies to data, not documents. Practically this means that if a customer’s personal data appears on a document along with business or other individuals’ data, the customer only has a right to receive their own personal data not that of the business or others. The Council may use discretion to provide additional information where it does not risk infringing upon the rights of others. Data also only needs to be provided once, for example if we have multiple instances of someone’s telephone number on different service accounts or letters, we only need to provide it one time.

Techniques such as redaction and extraction are commonly used for SARs to ensure only the personal information someone is entitled to is provided.

A SAR request relates to an individual. Joint requests, commonly submitted by couples, will be treated separately unless all data subjects expressly consent to receiving the information together. We will not accept one party requesting information on behalf of someone else without all subjects’ consent. Any concerns the Council has about the validity of the consent, such as fraud or coercion, will mean a request is rejected until the concerns are resolved.

Wherever possible we will provide SAR responses in a digital format to reduce the carbon impact, improve security, and reduce the cost of printing and postage.

Officers have access to additional resources to support the identification and processing of these requests on the intranet (search 'SAR'). The iGov officer will be informed of any SAR requests and manage them centrally. Individual services will be asked to locate and extract relevant data before the iGov officer sends a final response to the data subject.

All responses will include signposting to the privacy section of stroud.gov.uk and how to escalate the request if the data subject is unhappy with our management of it.

### Right of rectification

Everyone always has the right to ensure their personal data is accurate. This right is generally completed as part of our normal service delivery and where a data subject advises us of a valid inaccuracy, we will resolve it promptly.

### Right to be informed

Individuals may have a right to know how we process their information and why we need it. For our core services, the Council fulfils this with privacy notices, consent forms, signposting on websites and via temporary notices for one-off events. The privacy notices can be found at stroud.gov.uk/privacynotice and are updated whenever a service makes a change to processing.

Individuals do not have the right to be informed if their information is being processed for a purpose exempt from the GDPR. Most commonly this is for the prevention or detection of crime, as per the Data Protection Act 2018, Schedule 2.

### Right to erasure

An individual can request that their data be erased by an organisation. However, they must show that their right is greater than the organisations. Where there is a legal, contractual, or other legitimate reason to keep the data this will likely override the individual's request. For example:

**No right to erasure -** a Council tenant cannot request the landlord delete their personal data from a tenancy. Their tenancy contract overrides their request, and the Landlord needs to ensure accurate tenancy data for several purposes.

**Erasure request valid –** A member of the public made a complaint one year ago; they have now asked that we erase their personal data from the complaint file. In this instance an officer would check if the complaint needed to be kept for compliance purposes, if not and it was resolved satisfactorily, we would delete the data before the normal retention period as there is no reason to keep this personal data that overrides the request to delete it.

### Right to restrict processing and right to object

In certain circumstances individuals may request that an organisation ceases processing while a situation is resolved or request restrictions on how their data can be used.

The rights are commonly used together and mainly where a dispute in ongoing. The Council may, as part of a complaint or other investigation, stop the processing of personal data until matters are resolved. This right is subject to an assessment to judge whether the request outweighs the lawful reason to continue processing.

### Right to data portability

This right does not currently apply to any services in use by the Council. It is generally used in technological applications to allow for the sharing of information between platforms e.g. using a smartwatch and accessing its data on a smartphone or having your account information automatically moved over when switching banks.

### Rights related to automated processing

This right enables individuals to request a human intervention where a decision has been made solely by automated means. All decisions made by the Council currently have an element of human assessment, were this to change individuals would be fully informed on their rights. This is commonly used in automated credit checks.

## 5.6. Information Requests Procedure (Freedom of Information & Environmental Information Regulations)

As a public authority we are legally required to respond to valid public information requests. Requests generally fall into the categories of 'general' which will be dealt with under the Freedom of information Act 2000, or 'environmental' which will be dealt with under the Environmental Information Regulation 2004.

Generally, a request for information can be used where we have not proactively published information on stroud.gov.uk as part of our transparency work.

Officers will decide which legislation is most appropriate for the request based on the individual circumstances. All Council staff have access to proprietary guides on the intranet (search: FOI) and our regulator the ICO has a suite of reference documents to ensure a consistent approach to request management.

### What information is included?

It is important to understand that information requests only apply to information already held by, or on behalf of, the authority. In practice that means data we already have recorded somewhere. This can also include information provided to us by third parties and held by the authority. When working with businesses or other public authorities, officers must ensure the third party understands some information related to them may be disclosable. The legislation does not include information that has only been discussed verbally or is in essence 'in someone's head'. We have no requirement to create new information to satisfy an information request.

There are several exemptions to the legislation (FOI, EIR) which are designed to protect individual and commercial interests, privacy and other sensitive topics. We understand that requestors may not be aware of these exemptions and where we cannot provide information we will explain why and under which exemptions we are withholding data.

As the Council adheres to the data protection principles, we may have destroyed the information requested if it was no longer required to be kept for a specific lawful purpose.

### Responding to requests

We will always approach a request from the default position that we will publish the information requested and will then apply exemptions as appropriate. We will respond to most requests within 20 working days of receiving them. Occasionally we may need to query a request, and this will stop the request. If we have stopped the request, we will explain to the requestor why and what information is required to continue. We may stop a request to:

- Give a requestor opportunity to turn an invalid request into a valid one. Such as where no name is given on an FOI request, or where a request would exceed our FOI cost cap of 18 hours work to fulfil.
- To clarify the information requested if it is unclear or otherwise invalid.

As per the ICO's guidelines, we may treat any updated information as a new request with a refreshed 20 working day timescale to respond.

We can also extend the time to respond by up to a further 20 working day when we need to:

- To consider the public interest in disclosing information held by the authority for an FOI.
- The request is either complex, or the volume of the information makes it impracticable for us to comply with an EIR request.

We will always keep requestors informed if we need to stop a request or if a request may take additional time due to complexity or volume. If an extension is required, we will provide valid data to the requestor as soon as possible.

Once a request has been fulfilled, we will email the respondent directly and publish the request onto our website approximately one week after completion. We will remove requestor personal information from the website.

If a requestor is unhappy with how we have fulfilled a request they can make a complaint, otherwise known as an internal review, by following the instructions given at the end of the request reply.

### Common Exemptions and queries

The most common exemption we apply is the non-disclosure of personal information. As an information request is effectively published to the world at large, we will only provide personal information if it relates to a decision made by a Council officer in their professional capacity (e.g. a planning or policy decision) or is otherwise clearly in the public interest.

We also apply the ‘available by other means’ exemption frequently. As a local authority with limited resources, if a requestor can access information by reasonable other means we will direct them to do so and provide signposting to a relevant source wherever possible.

We will often use redaction and anonymisation for information requests to avoid the risk of harm to others. Where data has been redacted, we will explain in our reply why this is the case, and where it will not compromise the security of the redactions, we will provide a general explanation of the data we have removed.

We regularly receive requests of limited public interest asking for contact information of specific staff members, usually for sales. We will not provide names and direct contact details of staff outside of providing decision making evidence unless it is already clearly in the public domain. All procurement for the authority must be completed through the appropriate channels. We will usually guide requests of this nature to our senior leadership chart and ask that contact be made with the appropriate role through the standard contact channels.

## 5.7. Information Complaints

Complaints related to Information Governance, due to regulatory requirements, are managed slightly differently to corporate Council complaints. However, unless stated otherwise in this section, the approach and expectations of complaint management remain the same as the Councils Corporate Complaints Policy.

Complaint topics for iGov can include:

- Information request management
- Transparency code compliance
- Data breaches
- GDPR individual rights issues
- Data protection

If a complainant is dissatisfied with any Council matter covered by the Information Commissioners Office (ICO), they can make a complaint through any of our contact channels.

This complaint, or ‘Internal Review’ in the terminology of iGov, will be passed to the Information Governance Officer for investigation. The complaint will be reviewed and assessed against the ICO’s own guidance and expectations, referring to the relevant legislation and previous decisions. As there is only one complaints stage, these will be logged as a stage 1 complaint for statistical purposes.

A response will be issued to the complainant usually within 10 working days. Depending on the conclusions the response may explain why we are not changing a decision, or it may include additional information if we decide that the Council did not fulfil its obligations initially.

If following internal review the complainant remains dissatisfied, they may escalate the complaint to the ICO. This is managed in a similar way to Local Government Ombudsman complaints. The council will have the opportunity to defend or amend a decision and the DPO will lead Ombudsman complaints. The timescale to respond to the ICO is usually 10 working days. ICO Complaints will be logged as Ombudsman level for statistical purposes.

As with corporate complaints, the investigating officers may request consultation or evidence from the services involved in the complaint.

We are only required to begin complaints proceedings if a request for internal review is received within 40 working days of our original response. We may decide to take on a complaint over this limit if it is based on a strong, evidenced argument.

### 5.8. Records Retention & Management

Records are a specific collection of data held in any form. This could be anything from a note taken during a conversation, a housing tenancy database, a CCTV video recording, or a staff photograph. Each of us handles record management in our own lives, and it is not dissimilar in a business setting. We simply want to ensure the right records are in the right place, for the appropriate amount of time, then disposed of in the correct way.

This procedure is broken down into the key record management tasks of:

Creation

Access & Sharing

Retention

Each service of the Council is responsible for monitoring the records it holds and applying the appropriate actions to them at the appropriate time. This procedure provides overall guidance on best practice, and officers should consult with iGov if there is any concern about the most appropriate actions.

The Council has a retention schedule which lists all the key records and their retention actions, as well as best practice for what are called ‘unstructured’ records such as emails, notes, call recordings etc. This is found on stroud.gov.uk/privacynotice.

**Creation**

Records must be created for a specific purpose, and we should only collect the minimum data needed for that purpose. It is recommended that anytime a service wishes to create a new process, use a new system, or otherwise do something new with data that they consult across the organisation first to check if there is a suitable solution already available. It is also recommended to map out the expected flow of data for the process as this helps visualise what records are required and can identify any issues with the process. Officers can access specialist process mapping software to support this task, and they should contact the Policy & Governance team for support with this tool.

If the record contains **personal information**, you must apply the data protection principles to it. These will help ensure that your process is not only compliant with the law but also efficient and risk managed.

For **non-personal data records**, such as accounts or asset data, only information of value to the organisation or required under law should be included. This can reduce storage needs and improve efficiency by reducing the number of fields stakeholders must view and edit.

If the record is being created as part of a process involving **external third parties**, such as contractors, government, or charities you must comply with the data sharing procedure.

When creating a record, the format of it should be considered. Most Council data is digital, and officers and members should understand the audience for a record before saving it.

The .pdf format is most suitable for finished records that do not need editing, or that will be shared publicly. Saving in proprietary formats, such as .docx for Word or .xlsx for spreadsheets may not be accessible to persons not using Microsoft products. There are alternatives such as .rtf (rich text format) for word processing documents and .csv (comma separated values) for spreadsheets that are usable across different software.

When saving files, records should be stored in the smallest file format that still suits the purpose. For example, an officer should not save a video in 4k resolution when 1080p would be perfectly suitable for the purpose. Likewise, compressing pdfs and images is recommended when you do not need to print off documents. This is especially useful if you are required to share files. If you are unsure of the best ways to share data, see the access & sharing section below or contact the ICT team.

For older data or information collected in the field, paper copies can be saved as a digital image and archived to our imaging platform, or they can be typed up into a specific system. Original copies, unless legally required, should be destroyed via confidential waste once the digital version is saved.

As discussed elsewhere in this framework, avoid keeping data ‘just in case’. Every record should have a specific purpose.

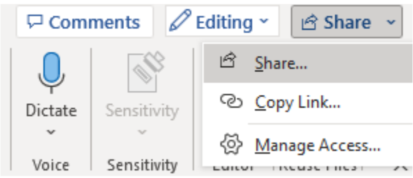
### Access & Sharing

Access to records should be on a ‘need to know’ basis. Managers are responsible for ensuring that only the required stakeholders have access to records and that access permissions are reviewed at least annually. This is especially important for leavers where access to data can be lost if adequate exit procedures and hand overs are not completed.

Changes to job roles, starters and leavers should all be updated to HR, ICT as well as any system owners to ensure accuracy and responsible systems control.

There are several ways to share data, officers should pick the most appropriate for their needs.

*Internal Sharing* – Internal sharing should be done using the inbuilt functions of MS365, including MS teams, where possible. You can usually find the sharing button in the top right corner of software such as Word and you can right-click any document you have uploaded to Teams or SharePoint for the same functionality.



We encourage staff to avoid emailing documents internally for a few key reasons:

1. When you email data, it is very hard to monitor the most up to date version if multiple people are editing separately. By using the MS365 sharing functions, every participant can edit or annotate the same document simultaneously. You also have full control over permissions, selecting who can edit, who can just view, and you can even block downloads.

2. Email is a key risk for data breaches. It is very easy to add a wrong recipient to an email, and once you have forwarded data you may not know what the recipients will do with it. Additionally, email is high risk for cyber-attack through phishing and malware sent as document links. The less we use it internally for sharing, the easier it is to spot these attacks.

*External Sharing* – For low-risk data, email can be used to share with external third parties where no alternative exists. If a third-party has a separate secure portal you are encouraged to use that method primarily. When emailing high-risk personal data, officers should encrypt the emails. For more information officers can search for ‘encryption’ on the intranet.

If you are using the services of a consultant, contractor or similar and you need to routinely share data, officers are encouraged to setup an MS365 team for the project and ICT can grant temporary, secure permissions for guests. This means they can quickly chat with you about issues, upload and share documents and ensure everyone is working off the same versions of records. Guests will only have access to the specific team group and once the relationship ends you can remove them or delete the whole group as required.

**Retention**

Whether a record contains personal information or not, we should generally only keep them for as long as they serve a purpose. Keeping records ‘just in case’ or beyond their use increases the risk they will be involved in a data breach, reduces productivity by increasing resource needed to search records, and increases storage costs.

The Councils retention schedule (pdf and spreadsheet copies available using this link) provides information on our key records as well as general advice. Broadly, records will be kept for as long as a relevant law dictates. If there is no specific law or best practice established related to a record, they will be kept under the limitations act for 6 years. Where the records are general in nature and do not relate to legal processes, decisions, or key actions they will be destroyed or anonymised once their purpose is served.

## 6. Local Government Transparency

As a local authority we publish certain information "to place more power into citizens’ hands to increase democratic accountability and make it easier for local people to contribute to the local decision-making process and help shape public services." (Local Government Transparency Code, 2015)

There are two main types of transparency data, those that are required by law and those which we choose to publish beyond these minimum standards.

The legal requirements make up the bulk of our published information, as these generally align with what is also in the public interest. By law we need to publish:

- Council & Committee meeting agendas, decisions, and minutes.
- Officer Decisions which affect the Council financially or where a council or committee has delegated responsibility.
- Registers for our Planning & Licensing decisions.
- Certain Public Notices.
- A range of transparency information defined under the Local Government Transparency Code.
- Council financial accounts.
- Election results.
- Public consultations.
- Councillor information and declarations of interest.
- And more which can all be found on stroud.gov.uk or by arranging an appointment to visit the Council offices.

In addition to our legal requirements, we may choose to publish additional information in response to public interest or for other legitimate reasons. These will be published in the most appropriate place, but most commonly on stroud.gov.uk and the Councils social media.

Where the Council receives enquiries for information already accessible by these means, or which is due to be published, customers will be signposted to the relevant webpage.

The Council will continually assess the data it is publishing and will add or remove information as necessary to satisfy public interest and the legal requirements of the transparency legislation. If officers identify additional data which could satisfy a public interest need, or which may reduce the burden on services by publication, they should contact their manager to assess the feasibility of adding it to our website. For example, if officers are receiving repeat FOI requests, they may consider whether publishing the information on a set schedule could alleviate some burden on limited staff resources.

# 7. Additional Guidance

## 7.1. Procurement, Contracts, and International Transfers

As part of any procurement or contract management, the responsible officer must ensure there are adequate data sharing and data protection clauses in place. Only the minimum amount of data required to fulfil the purpose should be shared.

Wherever possible data should only be shared within the UK or EU, as these areas both use GDPR. Some technologies may require sharing internationally outside of the EU and any such contracts must have a transfer risk assessment completed by iGov. If sharing data with the USA, the Data Protection (Adequacy) (USA) Regulations 2023 apply and only suppliers on the certified list should be used unless in exceptional circumstances.

It is not recommended to purchase or use any services or systems where data will be stored in a jurisdiction where data protection law is less robust than the GDPR. Officers should enquire with the iGov officer and/or DPO if there are any doubts.

When procuring systems, it is recommended that buyers scrutinise a system for how it will manage data. Procurers should consider:

- Can we reliably delete information once it has served a purpose and can we setup custom retention periods as necessary?
- What happens to the data at the end of a contract?
- How are user’s setup and permissions granted?
- Does the contract set out data protection requirements and responsibilities clearly?

If in doubt, procurers should contact iGov to discuss their options before anything is purchased.

### 7.2. The use of Artificial Intelligence

The Council is not averse to the use of innovative technologies when used responsibly and appropriately. The use of AI is not a replacement for the knowledge and experience of our officers and communities, but it can assist with existing work and idea generation.

If an AI tool is assessed to be the most suitable solution to a problem and provides the best value for money, it may be used under the following circumstances:

- No business or personal data should be entered into AI tools which use input data to develop a public model.
- Staff should use commercial grade versions of software which guarantee the confidentiality, integrity, and security of Council data.
- Anyone using generative-AI must understand that these are predictive models only and they can create biases and hallucinate facts.
- Any use of AI must be reviewed for errors and used only as an assistant to human critical analysis and experience.
- Anyone using AI should be aware of copyright and reference any sources responsibly.
- If any service wishes to procure or use a system which includes AI components, whether free or commercial, they must consult IT and iGov before any purchase or usage.
- Any use of AI or other digital tools is governed by this framework and the ICT policies. Users must consider data protection and appropriate security and record management.

Should the council ever develop AI solutions in house, it is recommended to use the Turing Institute's AI ethics and governance framework as a responsible guide.

## 8. Information Governance Resources, Training and Skills

Information Governance is a wide-ranging subject requiring knowledge of legislation and technology. Officers should seek support if they have any doubts about information governance elements of their work including in projects, contracts, or negotiations.

Guidance is available to Officers through the Council’s intranet and should be consulted in the first instance alongside this framework. Custom training can also be provided to suit the specific needs of services. Additionally, the iGov Officer, Data Protection Officer, and One Legal can provide specialist support and will keep up to date with the latest legislation and best practice changes.

All officers and members are required to complete annual data protection refresher training to evidence a level of competency in the management of data.

Approximately 50 officers take on additional duties to deliver our iGov obligations. This group respond to information requests, data protection requests, and fulfil our transparency requirements. To fulfil these roles, they are required to use a variety of skills and their support is invaluable as without them the Council would not be able to fulfil the significant number of information requests we receive each year.

## 9. Legislation

- Copyright, Designs & Patents Act 1988 – Defines copyright ownership, duration, and rights.
- Criminal Procedures and Investigations Act 1996 - In relation to disclosure rules,
- Data Protection Act (DPA) 2018 – Enacts the GDPR into law and outlines where it does not apply.
    - UK General Data Protection Regulation (GDPR) 2021 – Part of the DPA2018 which defines the general processing of personal data and sets out the rights of data subjects.
- Digital Economy Act 2017 – Defines government sharing of debt, fraud, and statistical information.
- Environmental information Regulations (EIR) 2004 - Provides public right of access to the environmental information held by public bodies.
- Equality Act 2010 – Defines protections from discrimination.
- Freedom of Information Act (FOIA) 2000 - Provides public right of access to information held by public bodies and defines code related to record management.
- Human Rights Act 1998 – Article 8: Respect for private and family life.
- Inspire 2009 – Defines the use and re-use of spatial data (GIS, Mapping, Location),
- Investigatory Powers Act (IPA) 2016 – Governs the use of communications metadata in investigations.
- Local Government Acts 1972, 1985, 1988, 1992 – Various acts defining responsibilities of local government.
- Local Government Transparency Code 2015 – Governs transparency requirements,
- Open Government License v3 – Defines the usage of data published under this license (transparency data, public information on storud.gov.uk).
- Public Records Acts 1958 & 1967 – Defines the archiving and access to certain public records after a period of 30 years.
- Regulation of Investigatory Powers Act (RIPA) 2000 – Governs the use of covert surveillance by public bodies.
- Re-use of Public Sector Information Regulations 2015 – Defines how public task information we hold the intellectual property rights to can be re-used.
- Surveillance Camera Code of Practice 2021 – Governs best practice for overt surveillance such as CCTV, Bodycams, and portable cameras.

## 10. Glossary

**Access Control –** The control over disclosure and access to information. This can be achieved through security (passwords, encryption), classification (Official-Sensitive, for SLT eyes only) and/or restriction (limiting access to certain seniority levels or specific teams through software policies)

**Aggregation [anonymisation] -** is a technique in which information is presented as totals or ranges, so that no information identifying individuals is shown. Small numbers in totals are a risk here and may need to be omitted or 'blurred' through random addition and subtraction.

**Anonymisation -** the process of removing, replacing and/or altering any identifiable information (identifiers) so that individuals cannot be identified.

**Data Controller –** The people or organisation who determine the purposes for which and the means by which personal data is processed. Generally the lead party in any contract, partnership, or project.

**Data Processor –** The people or organisations that process data on behalf of or under instruction of the data controller. Only processes data within established agreements. Normally suppliers of services.

**Data Protection Officer (DPO) -** A statutory role required under the GDPR as we are a public authority. The DPO is the authority on data protection matters of the Council.

**Data Subject -** A living individual to whom data relates.

**Incident Management -** is the process of handling incidents and breaches in a controlled way ensuring they are dealt with efficiently, with a consistent approach to ensure that any damage is kept to a minimum and the likelihood of recurrence is reduced by measures taken.

**Information Commissioners Officer –** The regulator for UK data protection and information governance services. They have powers to fine, demand rectification of breaches of legislation and bring criminal and civil enforcement measures against organisations.

**Information Governance –** The management of the use of information. At the Council it covers data protection, transparency including model publication, information requests including FOIA and EIR, as well as the processes and guidance in place to ensure all information is processed appropriately.

**Information Governance Officer –** Officer responsible for the operational management of the data protection, government transparency and information request services of the council. The usual point of contact for any enquiries related to information governance matters covered in this document.

**Lawful Basis –** Any processing of personal data must be justified with a specific lawful basis as defined in Article 6 of the UK GDPR. Most Council activities are performed as a public task as they are a statutory requirement. We explain the lawful basis for all our activities in the privacy notices at stroud.gov.uk/privacynotice. The six bases are:

Public Task (e.g. planning service), Legal Obligation (e.g. reporting fraud), Contract (e.g. tenancy agreement), Vital Interest (e.g. protecting someone from immediate harm), Legitimate Interest, Consent (e.g. for your photo to be taken at an event)

**Personal Data -** Any information relating to an identified or identifiable living natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

**Personal data breach** is defined as “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.” A breach is a type of security incident, however, the GDPR only applies where there is a breach of personal data. Near misses, are any kind of breach which could have occurred but was prevented by early intervention.

> **Confidentiality Breach** - A breach of confidentiality is when data or private information is disclosed to a third party without the data owner’s consent. Whether an intentional breach, accidental error or theft, the data owner may be entitled to take legal action for potential losses or damage that comes as a result of the breach of confidentiality.
>
> **Integrity Breach** - An integrity breach is where there is an unauthorised or accidental alteration of personal data.
>
> **Availability Breach** - An availability breach where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

**Primary use -** refers to the use of information for the purpose of delivering council services to individuals. This also includes relevant supporting administrative processes and audit/assurance of the quality of services provided. Primary use requires information at the person identifiable level.

**Privacy Notice** – A document which explains what personal information an organisation processes, why it needs it, who it shares data with, the rights of individuals and how to make a complaint about personal data. This complies with the individuals right to be informed and the lawful, fair, and transparent data protection principle. The notice is usually signposted to at the point we collect an individuals data.

**Processing -** Any operation or set of operations which is performed on data or on sets of data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**Pseudonymisation -** means the process of replacing personally identifiable information with an alternative non-person identifier. A coded reference, pseudonym or hash code are examples of pseudonymisation. Generally, a selected method is repeated across multiple data sets to facilitate aggregating data for research and statistics without identifying individuals. Care must be taken with this method to reduce risk of accidental identification through aggregated data.

**Publication –** The hosting of data in a public way such as on stroud.gov.uk, printed in a pamphlet, newsletter, press release or report to Committee/Council. Most Council data published is done so under the Open Government License and copyright and other laws still apply. The OLG does not apply to the use of personal data. While there may be grounds to publish data under specific license terms, this is practically impossible to enforce, and Officers should presume anything published will be accessible globally in perpetuity.

**Re-identification -** or de-anonymisation is where anonymised information is turned back into personal information using for example data matching or similar techniques. Where anonymisation is being undertaken, the process must be designed to minimise the risk of re-identification.

**Secondary use -** refers to the use of information about individuals for research purposes, audits, service management, commissioning, and contract monitoring and reporting. When PII is used for secondary uses the information should, where appropriate be limited and de-identified so that the secondary use process does not enable individuals to be identified.

**Special Category Data –** Personal data which needs additional protection and justification or usage because it is sensitive. Usage of this data requires an additional legal basis under article 9 of the GDPR. Includes:

- racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (where used for identification purposes), data concerning health, data concerning a person’s sex life, data concerning a person’s sexual orientation.

## 11. Document Control

| **Document Responsibility** | | |
|---|---|---|
| **Name** | **Document title** | **Service** |
| Owen Chandler | Information Governance Framework | Corporate Policy & Governance |

| **Document Version Control** | | | |
|---|---|---|---|
| **Date** | **Version** | **Issued by** | **Summary of changes** |
| 4th April 2024 | 1.3 | O. Chandler | Creation |

| **Policy Review** | | | |
|---|---|---|---|
| **Updating frequency** | **Review date** | **Person responsible** | **Service** |
| 4 Years – Full Review | April 2028 | Information Governance Officer | Corporate Policy & Governance |
| Annually – Legislation and best practice updates | April 2025 | Information Governance Officer | Corporate Policy & Governance |

| **Document Review and Approvals** | | |
|---|---|---|
| **Name** | **Action** | **Date** |
| Audit & Standards Committee | E.g. consulted, reviewed, approved | Date of review or approval |

STROUD DISTRICT COUNCIL
Council Offices • Ebley Mill • Ebley Wharf • Stroud • GL5 4UB
Telephone 01453 766321 • Facsimile 01453 750932
www.stroud.gov.uk

# AUDIT & STANDARDS COMMITTEE

# OFFICER REPORT

## Safeguarding Audit - Management Update

### 1. Introduction / Background

1.1 An internal audit was done by Audit Risk Assurance (ARA) on the SDC safeguarding framework and the report was produced in December 2023. The findings of the audit resulted in 14 recommendations, prioritised as follows: 2 High Priority; 10 Medium Priority; and 2 Low Priority. These are featured in the ARA report (Background Paper A).

1.2 Relating to the recommendations in the ARA report is a Management Action Plan which includes comments from the respective service manager and agreed action dates.

1.3 This Management Update will give insight into the actions carried out to date in respect of the recommendations.

### 2. Main Points

2.1 Recommendation 1 (High Priority): A risk management process has been created in the form of a risk register and is now being populated by respective service managers following the approval of the Councils new safeguarding policy and procedures guide (by CS&L Committee on 14 March 2024).

2.2 Recommendation 2 (High Priority): In unison with the development of a new safeguarding policy and procedures guide, a range of measures have been introduced with regards to the management of safeguarding training for staff and elected members. Essentially these measures focus on determining whether a staff member should complete safeguarding Level 3 training in addition to the mandatory Level 1 and 2 training. These include:

a) The staff Selected Candidate Form, used at recruitment stage to make an offer of employment to someone, has been amended to capture (from appointing managers) the level of safeguarding training required for each post.

b) The staff Induction Plan has been amended to ensure the correct safeguarding training level required for the post, is included. The respective manager will continue to ensure the training is completed as part of the probationary review. HR will continue to ensure all elements of the induction plan are completed before formally signing off a probationary review.

c) A master spreadsheet is being created by HR, to capture all requirements for safeguarding level 3 training. Support for this is coming from the Leadership Management Team (LMT) to define which current roles / members of staff are required to undertake Level 3 training. The aim is to have this task completed by the end of April 2024. The requirements for Disclosure Barring Service (DBS) checks and respective management, are being combined with this in one system.

2.3 Recommendation 3 (Medium Priority): A new Safeguarding Policy and Procedures Guide (Appendix B) has been developed in line with the Councils Policy Development and Review Framework and reflects our statutory duties as determined by legislation and national guidance. The guide was approved by Community Services and Licensing Committee on 14 March 2014.

2.4 Recommendation 4 (Medium Priority): Ubico give a presentation to new staff on their safeguarding responsibilities as part of their induction. Staff from SDC Community Services have set up a rota to ensure respective spot checks are being carried out on a quarterly basis, as part of a new monitoring system.

2.5 Recommendation 5 (Medium Priority): The HR service plan for 2024-2025 features a full HR policy review, to bring them in line with the Councils Policy Development and Review Framework. The DBS policy will be considered as part of this in the first quarter, with a completion expected by end of June 2024. Obtaining the correct data in respect of staffing and their roles, as outlined in 2.2, is required for the policy revision work to be accurate.

2.6 Recommendation 6 (Medium Priority): We are awaiting an update from Tara Skidmore on the progress of carrying out spot checks for DBS certification of housing contractors.

2.7 Recommendation 7 (Medium Priority): Services relating to the Canal Restoration Project and the Canal Engagement Project will carry out a review of DBS checks and their record keeping, once a review of the Council's DBS policy has been completed. Risk assessments will be updated once the policy and procedures have been completed.

2.8 Recommendation 8 (Medium Priority): A excel-based spreadsheet has been produced and is now functional, as the Corporate Safeguarding Group (CSG) Action and Decision-Making Log. This document is constantly 'live' in respect of the groups work and is used to capture and manage the actions and decisions of the group. It also includes a record of attendance at meetings for officers involved. Terms of Reference for the CSG have been updated since the approval of the policy and procedures guide (see 2.3) and these will be presented to the Strategic Leadership Team in July 2024.

2.9 Recommendation 9 (Medium Priority): The CSG agreed (on 28.03.24) that half yearly updates will be received by them on data, in reference to the following: concerns and incident reporting and referring; training participation and DBS checks. Further conversations with SLT will be held regarding how data is reported to the CS&L Committee.

2.10 Recommendation 10 (Medium Priority): Internal forms have been renamed as Report Forms to differentiate from that used for referrals. The matter of clarification on language, referencing internal and external safeguarding procedures and processes, has been addressed in the new policy and procedures guide (Background Paper B). The use of correct language (terminology) and familiarisation of correct procedures will be addressed via training and access to revised information on The Hub and Members Hub. A communication plan is being devised in which to introduce these revisions. The plan includes discussion by Leadership Management Team in quarter 1 of 2024/25 and an offer of bespoke support to service teams.

2.11 Recommendation 11 (Low Priority): A new Safeguarding Policy and Procedures Guide (Background Paper B) has been developed in line with the Councils Policy Development and Review Framework and reflects our statutory duties as determined by legislation and national guidance. The guide was approved by Community Services and Licensing Committee on 14 March 2014.

2.12 Recommendation 12 (Medium Priority): As stated in 2.2 and 2.3, the development of a new safeguarding policy and procedures guide highlights a range of measures being introduced with regards to the management of SDC's safeguarding responsibilities. The role of the Service Safeguarding Report Lead Officers and their respective services is stated in Background Paper B, Section 3.6. A record of community and customer facing services and corresponding Service Safeguarding Report Lead Officers, is being created in unison with the work by the HR Service to manage safeguarding training for staff and elected members. The aim is to have this task completed by the end of April 2024.

2.13 Recommendation 13 (Medium Priority): As stated in 2.5, the HR service plan for 2024-2025 features a full HR policy review, which includes the DBS policy. Obtaining the correct data from other services in respect of staffing and their roles is required for the policy revision work to be accurate. Support for this is coming from the Leadership Management Team (LMT) to define which current roles / members of staff are required to have DBS checks. The aim is to have this task completed by the end of June 2024.

2.14 Recommendation 14 (Low Priority): As stated in 2.3, a new Safeguarding Policy and Procedures Guide (Background Paper B) was approved by Community Services and Licensing Committee on 14 March 2014. The guide includes reference to those persons undertaking work experience with the Council, including workers aged under 18 and modern apprentices – see Section 3.8.5 of Background Paper B.

## 3. Conclusion

3.1 The recommendations in the Management Action Plan have either been completed or are progressing towards completion. The main points above highlight the work carried out since the ARA report was published. The Corporate Safeguarding Group acknowledge that there is more work involved in addressing all recommendations.

| | |
|---|---|
| **BACKGROUND PAPERS** | BP–A: Audit Risk Assurance Report<br>BP-B: Safeguarding Policy and Procedures Guide |
| **REPORT SUBMITTED BY** | Steve Miles, Youth Strategy and Safeguarding Manager |

This page is intentionally left blank

Bishop Fleming
Audit · Accountancy · Tax · Advisory

# External Audit Plan
# Stroud District Council

For the year ended 31 March 2024

# Contents

## Appendices

# Welcome

The purpose of this report is to give you an overview of the nature and scope of our audit work and bring to your attention the key aspects of the audit. The document also ensures that there is good communication between us, as auditors, and you.

If you have any queries regarding the plan, including the arrangements noted below, then please do not hesitate to contact us.

This Audit Plan has been prepared for the sole use of the management and those charged with governance of the Council. Except where required by law or regulation, this report should not be made available to any other parties without our prior written consent., No responsibilities are accepted by Bishop Fleming towards any party acting or refraining from action as a result of this plan.

We are issuing our 2023/24 External Audit Plan now, as it is our intention to issue your Audit Plan as close the year-end to which it relates, to ensure that there is timely discussion of the key areas of focus.  We are aware that your 2022/23 external audit has not yet been completed, so there may be some further changes to our approach, depending on the outcomes from that process. We will communicate any changes with you, as our audit progresses.

Alex Walling – Key Audit Partner

T: 0117 238 8838
E: awalling@bishopfleming.co.uk

# 1. General Audit Information

## 1.1. Engagement objectives and scope

The scope of our work is set in accordance with the National Audit Office's Code of Audit Practice (The Code) and the International Standards on Auditing (ISAs) (UK). Our work is planned to provide a focused and robust audit. We are required to provide an independent opinion as to whether the financial statements:

- give a true and fair view of the financial position of the Council at the year end and of its expenditure and income for the year then ended;
- have been prepared properly in accordance with the CIPFA/LASAAC Code of Practice on Local Authority Accounting in the United Kingdom 2023/24; and
- have been prepared in accordance with the requirements of the Local Audit and Accountability Act 2014.

Throughout the audit we will also ensure that, in line with the latest Auditing Standards, we communicate on a regular basis with those charged with governance.

We are also required to satisfy ourselves that the Council has made proper arrangements for securing economy, efficiency and effectiveness in its use of resources for the year ended 31 March 2024. The Code of Audit Practice requires us to report on the Council's arrangements under three specified reporting criteria:

- Financial sustainability – how the Council plans and manages its resources to ensure it can continue to deliver its services;
- Governance – how the Council ensures it makes informed decisions and properly manages its risks; and
- Improving economy, efficiency and effectiveness – how the Council uses information about its costs and performance to improve the way it manages and delivers its services.

The respective responsibilities of the audited body and the auditor are summarised in The Code. They are also set out in the PSAA Statement of Responsibilities of auditors and audited bodies issued by Public Sector Audit Appointments (PSAA), the body responsible for appointing us as your external auditor.

At the time of writing this Plan, there are a number of consultations ongoing. A Joint statement explaining the package of measures and how the various elements are intended to interact has been published on the Department for Levelling Up, Housing and Communities website. The outcomes of these consultations may impact on our audit plan and we will discuss any changes to our proposed work and timetable with management and the Audit and Standards Committee as events become clearer.

## 1.2. Audit reports

### Financial statements

On completion of our audit work on the financial statements, we will issue our Audit Completion Report to the Audit and Standards Committee, which will set out our findings.

In our audit report we will report on the basis under which the financial statements have been prepared and whether they give a true and fair view. The audit report will also:

- report on whether other information presented with the audited financial statements (for example, the Narrative Report and Annual Governance Statement) is materially consistent with the financial statements or our knowledge obtained in the audit; and
- conclude on the appropriateness of management's use of the going concern basis of accounting.

The form and content of our audit report may need to be amended in light of our audit findings.

We are required to report to you by exception the following matters, if:

- the Annual Governance Statement does not comply with "Delivering Good Governance in Local Government: Framework 2016 Edition" published by CIPFA/SOLACE; or
- we issue a report in the public interest under section 24 of the Local Audit and Accountability Act 2014; or
- we make a written recommendation to the Council under section 24 of the Local Audit and Accountability Act 2014 in the course of, or at the conclusion of the audit; or
- we make an application to the court for a declaration that an item of account is contrary to law under Section 28 of the Local Audit and Accountability Act 2014 in the course of, or at the conclusion of the audit; or
- we issue an advisory notice under Section 29 of the Local Audit and Accountability Act 2014 in the course of, or at the conclusion of the audit; or
- we make an application for judicial review under Section 31 of the Local Audit and Accountability Act 2014, in the course of, or at the conclusion of the audit.

Where no matters are identified, this will also be confirmed.

### Value for Money arrangements

On the completion of our work on whether the Council has made proper arrangements for securing economy, efficiency and effectiveness in its use of resources, we will issue our Auditor's Annual Report to the Audit and Standards Committee. This will provide a commentary on the Council's arrangements under the three specified criteria. The report will also set out whether any significant weaknesses were identified and any relevant recommendations.

## 1.3. Audit materiality

In planning and performing our audit work we will consider whether the financial statements are free from 'material misstatement'.

Materiality is an expression of the relative significance of a particular matter in the context of the financial statements as a whole. In general, misstatements, including omissions, are considered to be material if, individually or in aggregate, they could reasonably be expected to influence the economic decisions of users taken on the basis of the financial statements.

The assessment of whether a misstatement is material in the context of the financial statements is a matter of professional judgement and will have regard to both the size and the nature of the misstatement, or a combination of both. It is also affected by our perception of the financial information needs of users of the financial statements. Thus, different materiality levels may be appropriate when considering different aspects of the financial statements.

If there are any areas of specific concern in which you would like us to pay particular attention to then we will be pleased to discuss this with you, and whether our audit approach can be readily adapted to accommodate such a level in that area, or whether it will be more appropriate for a special exercise to be carried out on the area.

Our basis of materiality has been set as follows:

| | Basis of materiality |
|---|---|
| Stroud District Council | 2% of gross expenditure<br>This equates to £1.74m (based on the unaudited 2022/23 statement of accounts) |

Whilst the level of materiality is applied to the financial statements as a whole, we must also address the risk that any identified unadjusted audit differences are material when considered in aggregate. To reduce the risk of this being the case, we apply a lower level of materiality which we utilise within our work, known as Performance Materiality. This is set at a lower level than overall materiality and is determined by our assessment of the element of audit risk that pertains to the internal control environment of the Council.

## 1.4. Risk assessment and significant risks

### Financial statements

When planning our audit work, we will seek to minimise the risk of material misstatements occurring in the financial statements. To do this, we consider both the risk inherent in the financial statements themselves and the control environment in which the Council operates. We then use this assessment to develop an effective approach to the audit.

This risk assessment directs our testing towards the balances and transactions at the greatest risk of material misstatement so as to minimise the risk of undetected material misstatements. However, we do not test every group of transactions or balances but carry out sample testing of balances and transactions.

Therefore, there is an inherent and unavoidable risk that some material misstatements may not be detected and therefore audit procedures should not be relied upon to detect all material misstatements, fraud, irregularities or instances of non-compliance.

Based on our knowledge of the Council, we have identified the following as significant risk areas to be addressed during the audit. CIPFA LASAAC are consulting on temporary changes to the Code of Practice on Local Authority Accounting to reduce burdens on those who prepare and audit local body accounts. These proposed changes include simplifying the professional revaluation of operational property and reducing disclosure requirements around net pension assets and liabilities for at least 2 years. This may affect the significant risks we have currently identified and the approach we have proposed to address these risks. This is our initial assessment of audit risk based upon our work completed to date. Our conclusions may change, and additional risks may be identified as we complete additional planning procedures. We will provide the Audit and Standards Committee details of any changes in our risk assessments:

| Risk | Audit Approach |
|---|---|
| Management override of controls (required under the ISAs) | We are required by auditing standards (ISA 240) to consider fraud and management override of controls to be a significant risk for all audits as no matter how strong a control environment, there is the potential for controls to be overridden or bypassed. To address this risk, we will:<br>• Review the reasonableness of accounting estimates and critical judgements made by management;<br>• Test material journals processed at the year-end; and<br>• Test other journals with key risk attributes.<br>In testing journals, we will use data analytics tools to interrogate the whole population of journals posted in the year and focus on those with key risk factors. |
| Fraud in revenue recognition (required under the ISAs) | There is also a rebuttable presumption under auditing standards that revenue may be misstated due to improper recognition of revenue. This presumption may be rebutted if the auditor concludes that there is no risk of material misstatement due to fraud in revenue.<br>Having considered the risk factors set out in ISA240 and the nature of the revenue streams of the Council, we have concluded that the risk of fraud arising from revenue recognition can be rebutted because:<br>• There is little incentive to manipulate revenue recognition;<br>• Opportunities to manipulate revenue recognition are very limited; and<br>• The culture and ethical framework of local authorities, including Stroud District Council, mean that all forms of fraud are seen as unacceptable. |
| Fraud in expenditure recognition | Practice Note 10: Audit of Financial Statements and regularity of public sector bodies in the United Kingdom sets out that the risk of fraud related to expenditure is also relevant. We therefore need to consider whether we have any significant concerns about fraudulent financial reporting of expenditure which would need to be treated as a significant risk for the audit.<br>We do not consider this to be a significant risk for Stroud District Council because:<br>• Expenditure is well controlled, and the Council has a strong control environment; and<br>• The Council has clear and transparent reporting of its financial plans and financial position. |
| Valuation of land and buildings (and Council Dwellings) | There is a risk over the valuation of these assets due to the values involved and the high degree of estimation uncertainty, due to the sensitivity of the estimate to changes in key assumptions and judgements. To address this risk, we will:<br>• Document our understanding of the processes and controls put in place by management, and evaluate the design of the controls;<br>• Review the instructions provided to the valuer and the valuer's skills and expertise, in order to determine if we can rely on the management expert;<br>• Write to the valuer to confirm the basis on which the valuation was carried out;<br>• Confirm that the basis of valuation for assets valued in year is appropriate based on their usage;<br>• Review the appropriateness of assumptions used in the valuation of land and buildings. For assets not formally revalued in the year we will assess how |

| Risk | Audit Approach |
|---|---|
| | management has satisfied itself that these assets are not materially different from the current value at the year-end;<br>• Review accuracy and completeness of information provided to the valuer, such as floor areas;<br>• Test a sample of revaluations made during the year to ensure that they have been input correctly into the Council's asset register; and<br>• Form our own expectations regarding the movement in property values and comparing this to the valuations reflected in the Council's financial statements, following up valuation movements that appear unusual. |
| Valuation of the pension fund net liability | There is a risk over the valuation of the pension fund net liability due to the values involved and the high degree of estimation uncertainty, due to the sensitivity of the estimate to changes in key assumptions. To address this risk, we will:<br>• Document our understanding of the processes and controls put in place by management, and evaluate the design of the controls;<br>• Review the instructions provided to the actuary and the actuary's skills and expertise, in order to determine if we can rely on the management expert;<br>• Consider the accuracy and completeness of the information provided to the actuary;<br>• Ensure that the disclosures in the financial statements in respect of the pension fund liability are consistent with the actuarial report from the actuary;<br>• Carry out procedures to confirm the reasonableness of the actuarial assumptions made by reviewing the report of the consulting actuary (as auditor's expert) and performing any additional procedures suggested within the report; and<br>• Obtain assurances from the auditor of Gloucestershire Pension Fund in respect of the controls around the validity and accuracy of membership data, contributions data and benefits data sent to the actuary by the pension fund and the fund assets valuation in the pension fund financial statements. |

We will report back to you as part of our completion audit work, on the outcome of our work addressing these areas.

### Value for money arrangements

As part of our planning work, we have also considered whether there are any risks of significant weakness in the Council's arrangements for securing economy, efficiency and effectiveness in its use of resources that we need to perform further procedures on.

We have not identified any risks of significant weakness at this stage. We will consider the Auditor's Annual Report

We will keep our risk assessment under continual review and will consider the Auditor's Annual Report when that is issued by your predecessor auditor as part of that process. Any changes will be communicated to those charged with governance.

## 1.5. Control environment

Through our audit planning procedures, we will continue to develop our understanding of the control environment in which the Council operates.

At the time of issuing our Audit Plan our initial view is that the control environment in which the Council operates is effective and we will tailor our audit approach accordingly.

In the current year, we anticipate that our audit approach will focus on substantive procedures.

### 1.6. Adjusted and unadjusted items

Of the potential audit adjustments that we identify during our audit work, some may require adjustment. The decision to make an adjustment to the financial statements is one that the Council will need to make.

At the conclusion of the audit, we shall provide you with a schedule of potential adjustments that we identified during our audit work.

We will require you to confirm that you have considered the items and whether you have decided to adjust them in the financial statements; this will be included in the letter of representation.

We shall also provide you with a schedule, detailing those items that we identified during our audit work, which have not been adjusted for in the financial statements. This summary will not include errors that are 'clearly trivial', defined by us as those errors which individually account for no more than 5% of our materiality level.

We will require you to confirm that you have duly considered these unadjusted errors and that you have decided not to adjust for them in the financial statements; this will also be included in the letter of representation.

### 1.7. Fraud

While the Council has the ultimate responsibility for the prevention and detection of fraud, we are required to obtain reasonable assurance that the financial statements are free from material misstatement, including those arising as a result of fraud. Our audit approach includes the consideration of fraud throughout the audit, including making enquiries of management and those charged with governance.

### 1.8. Prior year recommendations

We will follow up on the progress made by the Council in addressing the recommendations made by the Council's previous auditor in respect of deficiencies reported in their ISA260 Audit Report.

## 2. The Audit Team

| | |
|---|---|
| Responsible individual: | Alex Walling |
| Email: | awalling@bishopfleming.co.uk |
| Manager: | Mark Bartlett |
| Email: | mbartlett@bishopfleming.co.uk |

# 3. Timetable

A full audit timetable has been included below:

**Stroud District Council**
YEAR END: 31 March 2024

| Date | Requirement |
|---|---|
| Feb - April 2024 | • Meetings with management<br>• Meetings with Chair of Audit and Standards Committee |
| March - April 2024 | Planning procedures, examining systems and controls in place. |
| Autumn 2024 | Review of predecessor auditor's files, which will be arranged when they have completed their 2022/23 work. |
| October 2024 | Audit fieldwork to be undertaken, completing work on significant risk areas and other material balances. |
| December 2024 | Audit completion meeting with year-end draft Audit Completion Report |
| January 2025 (TBC) | Audit and Standards Committee |

# 4. Audit Fees

Stroud District Council, in line with most other local government bodies, opted into the national scheme run by Public Sector Audit Appointments (PSAA) for the appointment of its external auditor for the five-year period with effect from 2023/24. PSAA set the scale fee for the audit of Stroud District Council under the contract. The audit scale fee set by PSAA for the Council and our proposed variations are set out below:

| | |
|---|---|
| PSAA scale fee 2023/24 | £148,896 |
| Proposed fee variations: | |
| ISA 315 | TBC |

The scale fees set by PSAA:

- are based on the expectation that complete and materially accurate financial statements, with supporting working papers, will be available within agreed timeframes (as set out in PSAA's Statement of Responsibilities document); and
- reflect as far as possible the predecessor auditor's previous assessment of audit risk and complexity.

Where work was substantially more or less than envisaged by the scale fee, we will propose that the fees should be varied. PSAA determine the outcome of any fee variations. The proposed fee variations set out above reflect issues that were not reflected in the scale fee when it was set by PSAA.

As the individual responsible for the project management of the audit, Mark Bartlett will monitor the position in relation to any issues that could potentially give rise to a fee variation and discuss them with the Chief Finance Officer/s.151 officer at the earliest opportunity.

There are no non-audit fees proposed at the planning stage.

ISA 315

The proposed fee variation in relation to ISA 315 is in respect of a significant change to auditing standards that applied for the first time for your audit for the year ended 31 March 2023. Due to the timing of the tender process, the impact of this has not been built into the audit scale fees.

In summary the main changes were as follows:

- The introduction of five new inherent risk factors to aid in risk assessment; subjectivity, complexity, uncertainty, change, and susceptibility to misstatement due to management bias or fraud.
- The introduction of a new spectrum of risk, at the higher end of which lie significant risks.
- The requirement for "sufficient, appropriate" evidence to be obtained from risk assessment procedures as the basis for the risk assessment.
- The introduction of more requirements in relation to gaining an understanding of the entity's IT environment, including requirements to identify and assess risks of material misstatement arising from the use of IT related to the IT application and other aspects of the entity's IT environment.

# 5. Ethical Issues

In order to comply with professional and ethical standards we are required to communicate to you all significant facts and matters that, in our professional judgement, may affect the firm's independence. This is for reference only, and unless you wish to make any comments, there is no need to respond.

## 5.1. Threats & safeguards

The standards require us to consider the perceived potential threats to our objectivity and independence in carrying out the audit. We are not providing any other audit related or non-audit related services. We have not identified any threats to the firm's independence.

## 5.2. Overall assessment

We can confirm that we comply with the Financial Reporting Council's (FRC) Ethical Standard and are able to issue an objective opinion on the financial statements. There are no significant facts or matters that impact on our independence as auditors that we are required or wish to draw to your attention.

## 5.3. Maintaining objectivity & independence

As a firm we have policies and procedures in place to monitor auditor objectivity and independence on a regular basis. If any additional threats are identified, we will of course advise you immediately.

We also perform an annual review of completed audit engagements for quality control purposes.

If you would like to discuss any of the above, please contact us.

# Appendices

# 1. Required communications with the Audit and Standards Committee

Under the auditing standards, there are certain communications that we must provide to the Audit and Standards Committee as those charged with governance. These include:

| Required communication | Where addressed |
|---|---|
| Our responsibilities in relation to the financial statement audit and those of management and those charged with governance. | Audit Plan |
| The planned scope and timing of the audit including any limitations, specifically including with respect to significant risks. | Audit Plan |
| With respect to misstatements:<br>• uncorrected misstatements and their effect on our audit opinion;<br>• the effect of uncorrected misstatements related to prior periods;<br>• a request that any uncorrected misstatement is corrected; and<br>• in writing, corrected misstatements that are significant. | Audit Completion Report |
| With respect to fraud communications:<br>• enquiries of those charged with governance to determine whether they have a knowledge of any actual, suspected or alleged fraud affecting the entity;<br>• any fraud that we have identified or information we have obtained that indicates that fraud may exist; and<br>• a discussion of any other matters related to fraud. | Audit Completion Report<br>Discussions at audit committees |
| Significant matters arising during the audit in connection with the entity's related parties. | Audit Completion Report |
| Significant findings from the audit including:<br>• our view about the significant qualitative aspects of accounting practices including accounting policies, accounting estimates and financial statement disclosures;<br>• significant difficulties, if any, encountered during the audit;<br>• significant matters, if any, arising from the audit that were discussed with management;<br>• written representations that we are seeking;<br>• expected modifications to the audit report; and<br>• other matters significant to the oversight of the financial reporting process or otherwise identified during the audit that we believe will be relevant to the Committee when fulfilling their responsibilities. | Audit Completion Report |
| Significant deficiencies in internal controls identified during the audit. | Audit Completion Report |
| Where relevant, any issues identified with respect to authority to obtain external confirmations or inability to obtain relevant and reliable audit evidence from other procedures. | Audit Completion Report |
| Audit findings regarding non-compliance with laws and regulations | Audit Completion Report<br>Discussions at audit committees |
| Significant matters in relation to going concern. | Audit Completion Report |
| Indication of whether all requested explanations and documents were provided by the entity. | Audit Completion Report |
| Confirmation of independence and objectivity of the firm and engagement team members. | Audit Plan<br>Audit Completion Report |

Bishop Fleming

Audit · Accountancy · Tax · Advisory

This document is confidential to: Stroud District Council

Bishop Fleming is a trading name of Bishop Fleming LLP, a limited liability partnership registered in England and Wales No. OC391282, and Bishop Fleming Bath Limited, a limited company registered in England and Wales No. 07869428. Registered offices: Stratus House, Emperor Way, Exeter Business Park, Exeter, Devon, EX1 3QS. A list of members' names for the LLP is available at the above address.

ICAEW CHARTERED ACCOUNTANTS

KRESTON UK

# STROUD DISTRICT COUNCIL

## AUDIT AND STANDARDS COMMITTEE

## 16 APRIL 2024

| | |
|---|---|
| **Report Title** | **Counter Fraud and Anti-Corruption Policy** |
| **Purpose of Report** | To present the Audit and Standards Committee an updated Counter Fraud and Anti-Corruption Policy for approval and adoption. |
| **Decision(s)** | **The Committee RESOLVES to:**<br>**(a) Approve and adopt the Policy attached to this report and;**<br>**(b) Authorises the Strategic Director of Resources to approve future minor amendments to the Policy in consultation with the Counter Fraud and Enforcement Unit and One Legal.** |
| **Consultation and Feedback** | Any Policies drafted or revised by the Counter Fraud and Enforcement Unit have been reviewed by One Legal and have been issued to the relevant Senior Officers, Management and Governance Officers for comment. |
| **Report Author** | Emma Cathcart, Head of Service,<br>Counter Fraud and Enforcement Unit<br>Email: Emma.Cathcart@cotswold.gov.uk |
| **Options** | The service is a specialist criminal enforcement service working with the Gloucestershire Local Authorities, West Oxfordshire District Council and the Policies are introduced across the Partnership. |
| **Background Papers** | None. |
| **Appendices** | Appendix 1 - Counter Fraud and Anti-Corruption Policy. |

| **Implications (further details at the end of report)** | Financial | Legal | Equality | Environmental |
|---|---|---|---|---|
| | Yes | Yes | Yes | No |

## 1. INTRODUCTION / BACKGROUND

1.1. Stroud District Council has joined the Counter Fraud and Enforcement Unit Partnership and as such a number of Policies and Strategies will be introduced.

1.2. The Counter Fraud and Enforcement Unit is tasked with reviewing the Council's Counter Fraud and Anti-Corruption Policy. It is recommended good practice that the Policy is updated and reviewed at least every three years or more frequently in line with any legislative changes.

1.3. In administering its responsibilities, the Council has a duty to prevent fraud and corruption, whether it is attempted by someone outside or within the Council such as another organisation, a resident, an employee or Councillor.

1.4. The Council is committed to an effective counter fraud and corruption culture, by promoting high ethical standards and encouraging the prevention and detection of fraudulent activities, thus supporting corporate and community plans.

## 2. MAIN POINTS

2.1. The Policy, attached at Appendix 1, was updated in 2022, in accordance with the Counter Fraud and Enforcement Unit Partnership review period.

2.2. The Policy was originally developed to reflect (i) latest legislation and (ii) the changes from the creation of the Single Fraud Investigation Services (operated by the Department for Work and Pensions) which subsumed the Council's responsibilities for investigating Housing Benefit Fraud.

2.3. The Policy was previously reviewed following the changes brought about by data protection legislation / regulations.

2.4. The Policy highlights the key legislation and roles and responsibilities of Councillors, Officers and other parties.

2.5. In 2022, a section was inserted relating to Money Laundering and Proceeds of Crime and relating to Modern Slavery, detailing the Council's responsibilities.

2.6. The Policy was also refreshed to reflect the growth of the Counter Fraud and Enforcement Unit work streams and responsibilities relating to risk.

2.7. As part of the consultation process, the Policy has been reviewed by One Legal, the Strategic Director of Resources and the Monitoring Officer.

2.8. Awareness will be raised with all staff following the approval of the Policy and refresher training in relation to counter fraud will be introduced following approval of the Policy.

## 3. CONCLUSION

3.1 The Policy has been reviewed to ensure the content reflects current legislation and the Council's Policies and Procedures. The Policy will replace the existing Counter Fraud and Anti-Corruption Policy.

## 4. IMPLICATIONS

### 4.1 Financial Implications

4.1.1 There are no direct financial implications as a result of this report.

4.1.2 The support of the Counter Fraud and Anti-Corruption Policy will help to support the prevention and detection of misuse of public funds and fraud therefore reducing potential financial loss to the Council.

Andrew Cummings, Strategic Director of Resources
Email: andrew.cummings@stroud.gov.uk

### 4.2 Legal Implications

4.2.1 In general terms, the existence and application of an effective fraud risk management regime assists the Council in effective financial governance which is less susceptible to legal challenge.

4.2.2 The legislation utilised by the Counter Fraud and Enforcement Unit and other service areas within the Council is identified within the Policy and the Council must comply with all legislative requirements.

4.2.3 The Council has a statutory obligation for enforcing a wide range of legislation, where it is necessary and proportionate to do so. Human rights implications are a consideration of this type of activity and this is included within any Policy and decision making.

One Legal
Email: legalservices@onelegal.org.uk

### 4.3 Equality Implications

4.3.1 The promotion of effective counter fraud controls and a zero tolerance approach to internal misconduct promotes a positive work environment.

### 4.4 Environmental Implications

4.4.1 There are no significant implications within this category.

This page is intentionally left blank

Agenda Item 9

Appendix 1

# Counter Fraud and Anti-Corruption Policy

| **Version Control:** | |
|---|---|
| **Document Name:** | Counter Fraud and Anti-Corruption Policy |
| **Version:** | 2.1 |
| **Responsible Officer:** | Emma Cathcart, Counter Fraud and Enforcement Unit |
| **Approved by:** | Executive / Cabinet / Audit & Standards Committee |
| **Next Review Date** | May 2025 |
| **Retention Period:** | N/A |

## Revision History

| **Revision date** | **Version** | **Description** |
|---|---|---|
| August 2019 | 1.1 | Update following changes to data protection legislation |
| May 2022 | 2 | Review and Update |
| December 2023 | 2.1 | Inclusion of Stroud DC |

## Consultees

| **Internal** | **External** |
|---|---|
| CFEU Partnership Board | |
| One Legal / Legal Services | |
| Audit Committee / Audit and Governance Committee / Audit, Compliance and Governance Committee | |

## Distribution

| **Name** | |
|---|---|
| All Staff | |

**CONTENTS**

## 1. INTRODUCTION AND PURPOSE OF THE POLICY

1.1. In administering its responsibilities; this Council has a duty to prevent fraud and corruption, whether it is attempted by someone outside or within the Council such as another organisation, a resident, an employee or Member. The Council is committed to an effective Counter Fraud and Anti-Corruption culture, by promoting high ethical standards and encouraging the prevention, detection and investigation of fraudulent activities.

1.2. The Section 151 Officer has a statutory responsibility under Section 151 of the Local Government Act 1972 to ensure the proper arrangements for the Council's financial affairs to include the development of financial codes of practice and accounting instructions. Through delegation of duties, the Officer ensures appropriate controls are in place.

1.3. The Monitoring Officer has a statutory responsibility to advise the Council on the legality of its decisions and to ensure that the Council's actions do not give rise to illegality or maladministration. It is therefore essential for employees to follow the Council's policies and procedures to demonstrate that the Council is acting in an open and transparent manner.

1.4. The Council has a statutory duty to undertake an adequate and effective internal audit of its accounting records and its system of internal controls. The Council's Financial Rules state that 'whenever a matter arises which involves, or is thought to involve irregularities concerning cash, stores or other property of the Council, or any suspected irregularity in the exercise of the functions of the Council, the Director, Head of Service or equivalent Senior Officer has a duty to immediately notify the Section 151 Officer and the Monitoring Officer, who shall take steps as they consider necessary by way of investigation and report'. Furthermore the Financial Rules also state that each Director, Head of Service or equivalent Senior Officer is responsible for 'notifying the Section 151 Officer and the Chief Internal Audit Officer immediately of any suspected fraud, theft, irregularity, improper use or misappropriation of the Council's property or resources.

1.5. The Council has a zero tolerance approach to fraud committed or attempted by any person against the organisation or any of its partner agencies. The Council will thoroughly investigate all suggestions of fraud, corruption or theft, from within the Council and from external sources which it recognises can:

- Undermine the standards of public service that the Council is attempting to achieve by diverting resources from legitimate activities.
- Reduce the level of resources and services available for the residents of the borough, district or county as a whole.
- Result in consequences which damage public confidence in the Council and / or adversely affect staff morale.

1.6. Any proven fraud will be dealt with in a consistent and proportionate manner. Appropriate sanctions and redress for losses will be pursued, to include criminal proceedings against anyone perpetrating, or seeking to perpetrate, fraud, corruption or theft against the Council.

1.7. The Council is committed to the highest possible standards of openness, probity, honesty, integrity and accountability. The Council expects all Officers, Members and partner organisations to observe these standards and values, which are defined within the Code of Conduct for Employees and the Members Code of Conduct, to help achieve the Council's over-arching priority for the continued delivery of outcomes and value for money for local tax-payers.

## 2. DEFINITIONS

2.1. **FRAUD**

The term “fraud” is usually used to describe depriving someone of something by deceit, which might either be misuse of funds or other resources, or more complicated crimes like false accounting or the supply of false information. In legal terms, all of these activities are the same crime, theft, examples of which include deception, bribery, forgery, extortion, corruption, theft, conspiracy, embezzlement, misappropriation, false representation, concealment of material facts and collusion.

2.2 Fraud was introduced as a general offence and is defined within The Fraud Act 2006. The Act details that a person is guilty of fraud if he commits any of the following:

- Fraud by false representation; that is if a person:

(a) dishonestly makes a false representation, and
(b) intends, by making the representation:
(i) to make a gain for himself or another, or
(ii) to cause loss to another or to expose another to a risk of loss.

- Fraud by failing to disclose information; that is if a person:

(a) dishonestly fails to disclose to another person information which he is under a legal duty to disclose, and
(b) intends, by failing to disclose the information:
(i) to make a gain for himself or another, or
(ii) to cause loss to another or to expose another to a risk of loss.

- Fraud by abuse of position; that is if a person:

(a) occupies a position in which he is expected to safeguard, or not to act against, the financial interests of another person,
(b) dishonestly abuses that position, and
(c) intends, by means of the abuse of that position:
(i) to make a gain for himself or another, or
(ii) to cause loss to another or to expose another to a risk of loss.

2.3 In addition the Act introduced new offences in relation to obtaining services dishonestly, possessing, making, and supplying articles for the use in frauds and fraudulent trading applicable to non-corporate traders.

2.4. **CORRUPTION**

Is the deliberate use of one’s position for direct or indirect personal gain. “Corruption” covers the offering, giving, soliciting or acceptance of an inducement or reward, which may influence the action of any person to act inappropriately and against the interests of the organisation.

2.5. **THEFT**

Is the physical misappropriation of cash or other tangible assets. A person is guilty of “theft” if he or she dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it.

2.6. **MONEY LAUNDERING**

Money laundering is the process by which criminals attempt to 'recycle' the proceeds of their criminal activities in order to conceal its origins and ownership whilst retaining use of the funds.

2.7 The burden of identifying and reporting acts of money laundering rests within the organisation. Any service that receives money from an external person or body is potentially vulnerable to a money laundering operation. The need for vigilance is vital and any suspicion concerning the appropriateness of a transaction should be reported and advice sought from the Monitoring Officer, Section 151 Officer or Chief Internal Audit Officer. A failure to report a suspicion could compromise an individual and they could be caught by the money laundering provisions. All employees are therefore instructed to be aware of the increasing possibility of receiving requests that are not genuine and are in fact for the purpose of money laundering.

2.8 The Council recognises its responsibilities under Money Laundering and Proceeds of Crime Legislation. These responsibilities are adhered to in line with the Council's Proceeds of Crime and Anti-Money Laundering Policy and the related Procedures. The Council is required to have a designated Officer for money laundering reporting purposes. The officer nominated to receive disclosures about money laundering activity is the Officer appointed under section 151 of the Local Government Act 1972.

2.9 Both Financial and Legal Officers working for the Council also have their own professional guidance in relation to money laundering which places a duty on them to report any suspicions. These suspicions may override their legal professional privilege and confidentiality.

## 2.10 **BRIBERY**

The Bribery Act 2010 introduced four main offences, simplified below. Please note, a 'financial' or 'other advantage' may include money, assets, gifts or services within the following:

- Bribing another person: a person is guilty of an offence if he offers, promises or gives a financial or other advantage to another person. Further if he intends the advantage to induce a person to perform improperly a function or activity or if he knows or believes the acceptance of the advantage offered constitutes improper activity.
- Offences relating to being bribed: a person is guilty of an offence if he requests, agrees to receive, or accepts a financial or other advantage intending that as a consequence an improper activity or function will be performed improperly or if he knows or believes the acceptance of the advantage offered constitutes improper activity. Where a person agrees to receive or accepts an advantage as a reward for improper activity or function that has been performed. It does not matter whether the recipient of the bribe receives it directly or through a third party, or whether it is for the recipient's ultimate advantage or not.
- Bribery of a foreign public official: a person who bribes a foreign public official is guilty of an offence if the person's intention is to influence the foreign public official in their capacity, duty or role as a foreign public official. A person must also intend to obtain or retain business or an advantage in the conduct of business and must offer, promise or give any financial or other advantage.
- Failure of commercial organisations to prevent bribery: organisations, which include the Council, must have adequate procedures in place to prevent bribery in relation to the obtaining or retaining of business associated with the business itself.

2.11 The Council is committed to ensuring the prevention of corruption and bribery and sets out its policy in relation to the acceptance of gifts and hospitality by Officers and Members within the Codes of Conduct for Employees / Members (or equivalent) and the Constitution. Offers of or the receipt of any gifts or hospitality should be recorded by Officers and Members in the appropriate register whether accepted or refused. Officers and Members are also required to declare any outside interests that they have which may result in a conflict of interest in respect of transactions and dealings with the Council. Again, any such interests will be recorded in an appropriate register.

2.12 Prior to entering into any business arrangements, all Council Officers and/or business units should ensure that they have taken all reasonable steps to identify any potential areas of risk relating to bribery or corruption. If an Officer has any concerns they must raise them with The Chief Internal Audit Officer.

### 2.13. MODERN SLAVERY

Modern Slavery takes a number of forms but all relate to the illegal exploitation of people for personal or commercial gain. The Council recognises its responsibilities as outlined within the legislation and is committed to promoting transparency in supply chains to prevent modern slavery and to take appropriate action to identify and address those risks.

## 3. SCOPE

3.1 In relation to any of the above mentioned offences, this policy applies to:

- All employees, including shared service employees, casual workers and agency staff.
- Members.
- Committee Members of Council funded voluntary organisations.
- Partner organisations, where the Council has a financial or statutory responsibility.
- Council Suppliers, Contractors and Consultants.
- The general public.

## 4. AIMS AND OBJECTIVES

4.1 The aims and objectives of the Counter Fraud and Anti-Corruption Policy are to:

- Ensure that the Council has measures in place to guard against fraud and loss and that the Council maximises revenue recovery.
- Safeguard the Council’s valuable resources by ensuring they are not lost through fraud but are used for providing services to the community as a whole.
- Create a ‘counter fraud’ culture which highlights the Council’s zero tolerance to fraud, corruption, bribery and theft, which defines roles and responsibilities and actively engages everyone (the public, Members, Officers, managers and policy makers).

4.2 The Council aims to:

- Proactively deter, prevent and detect fraud, corruption, bribery and theft.
- Investigate any suspicions of, or detected instances of fraud, corruption, bribery and theft.
- Enable the Council to apply appropriate sanctions, to include prosecution, and recovery of losses.
- Provide recommendations to inform policy, system and control improvements, thereby reducing the Council’s exposure to fraudulent activity.

## 5. PRINCIPLES

5.1 The Council will not tolerate abuse of its services or resources and has high expectations of propriety, integrity and accountability from all parties identified within this policy. Maintaining this policy supports this vision.

5.2 The Council has a documented Constitution, Scheme of Delegated Powers and Financial Regulations to give Members and Officers clear instructions or guidance for carrying out the Council's functions and responsibilities. Responsibility for ensuring compliance with these documents rests with management with adherence being periodically monitored by Internal Audit Services. Where breaches are identified these will be investigated in accordance with this policy and the Council's Financial Rules.

5.3 The Council expects that Members and Officers will lead by example in ensuring adherence to rules, procedures and recommended practices. A culture will be maintained that is conducive to ensuring probity. Members and Officers should adopt the standards in public life as set out by the Nolan Committee, known as the Nolan Principles:

- Selflessness – to take decisions solely in terms of the public interest and not in order to gain for themselves.
- Integrity – not to place themselves under any obligation to outside individuals or organisations that may influence the undertaking of their official duties.
- Objectivity – when carrying out any aspect of their public duties, to make decisions and choices on merit.
- Accountability – to be accountable, to the public, for their decisions and actions and must submit themselves to the appropriate scrutiny.
- Openness – to be as open as possible about the decisions and actions they take and the reasons for those decisions and actions. The dissemination of information should only be restricted when the wider public interest clearly demands it.
- Honesty – to declare any private interests which relate to their public duties and take steps to resolve any conflicts arising in a manner which protects the public interest.
- Leadership – to promote and support these principles by leadership and example.

5.4 The Council will ensure that the resources dedicated to counter fraud activity are appropriate and any officers involved in delivering these services are trained to deliver a professional counter fraud service to the correct standards ensuring consistency, fairness and objectivity.

5.5 All fraudulent activity is unacceptable, and may result in consideration of legal action being taken against the individual(s) concerned. In addition, the Council has in place disciplinary procedures which must be followed whenever Officers are suspected of committing a fraudulent or corrupt act. These procedures are monitored and managed by the Human Resources Team and may be utilised where the outcome of an investigation indicates fraudulent or corrupt acts have occurred.

5.6 The Council may pursue the repayment of any financial gain from individuals involved in fraud, malpractice and wrongdoing. The Council may also pursue compensation for any costs it has incurred when investigating fraudulent or corrupt acts.

5.7 This policy encourages those detailed within this document to report any genuine suspicions of fraudulent activity. However, malicious allegations or those motivated by personal gain will not be tolerated and, if proven, disciplinary or legal action may be taken. Reporting arrangements in relation to incidents of fraud or irregularity are detailed below.

5.8 The Council will work both internally across different departments and with external organisations such as the Police, HM Revenue and Customs and other Councils to strengthen and continuously improve its arrangements to prevent fraud and corruption. The Council is committed to assisting the Police in fighting Serious and Organised crime and will implement measures and share data to ensure the Council is not engaging with organised crime gangs when procuring goods and services.

5.9 The Council collects and stores data within multiple departments to enable data cleansing, data sharing and data matching. This process can be utilised for the prevention and detection of fraud and the Council will pursue this where appropriate. The Council applies fair processing practices and these are reflected within data collection documents, stationery and other data collection processes such as those required for the National Fraud Initiative.

5.10 The Council will ensure Members and Officers receive the appropriate training relating to the areas covered within this Policy.

## 6. RESPONSIBILITIES

| OFFICER / DEPARTMENT | SPECIFIC RESPONSIBILITIES |
|---|---|
| **Head of Paid Service / Chief Executive** | Ultimately accountable for the effectiveness of the Council's arrangements for countering fraud and corruption. |
| **Chief Finance Officer**<br>**(Section 151 Officer)** | To ensure the Council has adopted an appropriate Counter Fraud and Anti-Corruption Policy. That there is an effective internal control environment in place and resources to investigate allegations of fraud and corruption. |
| **Monitoring Officer** | To advise Members and Officers on ethical issues, conduct and powers to ensure that the Council operates within the law and statutory Codes of Practice. |
| **Audit Committee/ Audit and General Purposes Committee / Audit and Governance Committee / Audit and Standards Committee** | To receive formal assurance from an appropriate representative at meetings and an annual opinion report in relation to the Council's control measures and counter fraud activity.<br>The Audit Committee also receives assurance from external audit on the Council's Annual Accounts and Annual Governance Statement. |
| **Councillors / Members** | To comply with the Members Code of Conduct and related Council policies and procedures.<br>To be aware of the possibility of fraud, corruption, bribery and theft and to report any genuine concerns to the Chief Internal Audit Officer. |

| OFFICER / DEPARTMENT | SPECIFIC RESPONSIBILITIES |
|---|---|
| **External Audit / Internal Audit** | Has a duty to ensure that the Council has adequate arrangements in place for the prevention and detection of fraud, corruption, bribery and theft.<br>Has powers to investigate fraud and the Council may invoke this service. |
| **Counter Fraud and Enforcement Unit** | Responsible for assisting the development and implementation of the Counter Fraud and Anti-Corruption Policy. The Counter Fraud Unit have a duty to monitor the investigation of any reported issues of irregularity.<br>To ensure that all suspected or reported irregularities are dealt with promptly and in accordance with this policy.<br>That action is identified to improve controls and reduce means, opportunity and the risk of recurrence.<br>Reporting to the appropriate Senior Officer(s) (Section 151 Officer, Monitoring Officer, Chief Internal Audit Officer) with regard to the progress and results of investigations.<br>Reporting annually to the Audit Committee on proven frauds. |
| **Counter Fraud Provision / Services** | To proactively deter, prevent and detect fraud, corruption, bribery and theft within or against the Council.<br>To work on behalf of charities, Social Housing Providers and other organisations to proactively deter, prevent and detect fraud, bribery, corruption and theft for the benefit of local residents and the public purse.<br>To investigate all suspicions of fraud, corruption, bribery or theft, within or against the Council, in accordance with the Criminal Procedures and Investigations Act 1996 (CPIA).<br>To consider reputational damage and the public interest test when investigating any instances of fraud, corruption, bribery or theft.<br>To conduct interviews under caution when appropriate in accordance with the Police and Criminal Evidence Act 1984 (PACE).<br>To undertake any surveillance operation or obtaining any communications data, adhering to the |

| OFFICER / DEPARTMENT | SPECIFIC RESPONSIBILITIES |
|---|---|
| | Regulation of Investigatory Powers Act 2000 (RIPA) and the Investigatory Powers Act 2016 – this is applicable when undertaking criminal investigations only.<br>To comply with Data Protection Legislation (and the General Data Protection Regulations) when obtaining or processing personal data.<br>To report to the appropriate Senior Officer(s) for decisions in relation to further action.<br>To enable the Council to apply appropriate sanctions, to include criminal proceedings, and to assist in the recovery of losses in accordance with the Council's Corporate Enforcement Policy. To include prosecutions on behalf of Social Housing Providers, Charities, and other organisations where it is in the public interest and for the benefit of the local residents.<br>To prepare Witness Statements and prosecution paperwork for the Council's Legal Department.<br>To attend and present evidence in the Magistrates Court, the Crown Court and Employment Tribunals.<br>To provide recommendations to inform policy, system and control improvements.<br>To provide fraud awareness training and updates for Members and Officers.<br>To publicise successes where appropriate. |
| **Human Resources** | To report any suspicions of fraud, corruption, bribery or theft to the Section 151 Officer, Monitoring Officer or Counter Fraud representative if reported directly to HR or if identified during any disciplinary or internal procedures.<br>To ensure recruitment procedures provide for the obtainment and verification of significant information supplied by applicants in accordance with the HR Vetting and Recruitment Fraud Risk Report. |
| **Strategic Directors, Heads of Service, Service Managers or equivalent Senior Officers** | The primary responsibility for maintaining sound arrangements to prevent and detect fraud and corruption rests with management.<br>To promote awareness and ensure that all suspected or reported irregularities are immediately referred to the appropriate Senior Officer.<br>To ensure that there are mechanisms in place within their service areas to assess the risk of fraud, corruption, bribery and theft. To reduce these risks |

| OFFICER / DEPARTMENT | SPECIFIC RESPONSIBILITIES |
|---|---|
| | by implementing internal controls, monitoring of these controls by spot checks and to rectify weaknesses if they occur. |
| **Staff / Employees / Officers** | To comply with Council policies and procedures when conducting their public duties.<br>To be aware of the possibility of fraud, corruption, bribery and theft and to report any genuine concerns. Officers may report suspicions as detailed below.<br>Referrals can also be made in confidence in accordance with the Council's Whistleblowing Policy. |
| **Public, Partners, Suppliers, Contractors and Consultants** | To be aware of the possibility of fraud and corruption within or against the Council and to report any genuine concerns or suspicions as detailed below. |

## 7. APPROACH TO COUNTERING FRAUD

7.1 The Council has a responsibility to reduce fraud and protect its resources by enabling counter fraud services to complete work in each of the following key areas:

### 7.2 DETERRENCE

The best deterrent is the existence of clear procedures and responsibilities making fraud and corruption difficult to perpetrate and easy to detect. As detailed already within this policy, the Council has a number of measures in place to minimise risk:

- Clear codes of conduct for Officers and Members.
- Register for declarations of interest / gifts and hospitality for Members and Officers.
- Clear roles and responsibilities for the prevention and detection of fraud, corruption, bribery and theft including an Audit Committee, an appointed Monitoring Officer, Section 151 Officer and trained Counter Fraud Officers.
- Effective ICT security standards and usage policies.
- The application of appropriate sanctions and fines as detailed below.

7.3 The existence of an effective Counter Fraud Team is a prime deterrent for fraud and corruption. Counter Fraud Officers and the Internal Audit Team analyse and identify potential areas at risk of fraudulent abuse with the assistance of the Council's Corporate Management, efficient and effective audits of principal risk areas can then be conducted.

7.4 The Council will promote and develop a strong counter fraud culture, raise awareness and provide information on all aspects of its counter fraud work. This may include advice on the intranet, fraud e-learning tools, publicising the results of proactive work, investigating fraud referrals and seeking the recovery of any losses.

7.5 **PREVENTION**

The Council will strengthen measures to prevent fraud ensuring consideration of the Fraud Risk Strategy, associated documents and fraud risk register. Counter Fraud Officers will work with management and policy makers to ensure new and existing systems, procedures and policy initiatives consider any possible fraud risks. Any internal audit conducted will also consider fraud risks as part of each review and ensure that internal controls are in place and maintained to combat this.

7.6 Important preventative measures include effective recruitment to establish the propriety and integrity of all potential employees as set out within the HR Vetting and Recruitment Fraud Risk Report. Recruitment is carried out in accordance with the Council's Recruitment and Selection Policy and provides for the obtainment and verification of significant information supplied by applicants.

7.7 The Council will undertake any internal remedial measures identified by any investigation to prevent future recurrence at the first opportunity.

7.8 **DETECTION**

A record of fraud referrals received will be maintained by Counter Fraud Officers (and other departments as applicable). This record helps to establish those areas within the Council most vulnerable to the risk of fraud. In addition, a consistent treatment of information and independent investigation is ensured. A Council wide fraud profile is created which then informs any detailed proactive work.

7.9 The Council is legislatively required to participate in a national data matching exercise; the National Fraud Initiative (NFI). Particular sets of data are provided and matched against other records held by the Council or external organisations. Where a 'match' is found it may indicate an irregularity which requires further investigation to establish whether fraud has been committed or an error made. An officer within the authority is designated as the 'Key Contact' for this process. The initiative also assists in highlighting areas which require more proactive investigation. The Council may engage in other data matching/sharing for the purposes of fraud prevention and detection, and for the recovery of monies owed.

7.10 Safeguarding and deterrent internal controls and monitoring procedures are established for financial and other systems within the Council, for example those set out within the Council's Financial Rules / Contract Rules.

7.11 The Council relies on employees, Members and the public to be alert and to report any suspicions of fraud and corruption which may have been committed or that are allegedly in progress. Managers should be vigilant and refer any matters which may require additional monitoring to a senior representative within the Human Resources Department for guidance and further action.

7.12 **INVESTIGATION**

The Council will investigate all reported incidents of fraud or irregularity using its counter fraud resources. The Council will ensure the correct gathering and presentation of evidence in accordance with the Criminal Procedures and Investigations Act 1996.

7.13 Investigations will make due reference to Employment Law as necessary and be conducted within a reasonable time in accordance with the Human Rights Act 1998. Investigations will also adhere to and comply with other applicable legislation such as the Police and Criminal Evidence Act 1984, Data Protection Legislation and the Freedom of Information Act 2000 as appropriate.

7.14 Officers may utilise investigative tools and gain intelligence utilising a number of legal gateways and data sharing agreements. This may include membership to third party organisations such as the National Anti-Fraud Network (NAFN).

7.15 When investigating allegations of fraud and corruption, the Council may be required to conduct surveillance. The Council must comply with the Regulation of Investigatory Powers Act 2000 which ensures that investigatory powers are used in accordance with human rights. To ensure compliance the Council has a written procedure detailing who may authorise covert surveillance and the use of covert human intelligence sources. Standard documentation has been adopted which must be used by an Officer when seeking such authorisation.

7.16 Officers may also need to acquire communications data when conducting an investigation. This is permissible however; the Council must adhere to the Investigatory Powers Act 2016 when applying for this information and the correct nominated single point of contact must be used. As above, specific details are set out within the written procedures.

7.17 The Counter Fraud and Enforcement Unit Officers adhere to the appropriate legislation when investigating irregularities and allegations of fraud. This includes the need to:

- Deal promptly with the matter.
- Record all evidence received.
- Ensure that evidence is sound and adequately supported.
- Conduct interviews under caution when necessary.
- Ensure security of all evidence collected.
- Contact other agencies if necessary e.g. Police, Trading Standards, HM Revenue and Customs.
- Notify the Council's insurers.
- Implement Council disciplinary procedures where appropriate.
- Attend court and present evidence.

7.18 **SANCTIONS**

The Council will apply considered sanctions to individuals or organisations where an investigation reveals fraudulent activity. This may include:

- Appropriate disciplinary action in line with the Disciplinary Policy.
- Fines and penalties.
- Criminal proceedings.
- Civil proceedings to recover loss.

7.19 **REDRESS**

A crucial element of the Council's response to tackling fraud is seeking financial redress. The recovery of defrauded monies is an important part of the Council's strategy and will be pursued in line with internal debt recovery processes and legal redress i.e. Confiscation Orders and the application of the Proceeds of Crime Act 2002.

7.20 **CONTROL FAILURE RESOLUTION**

In addition to the above, Internal Audit also prepares a risk based annual Audit Plan that details the key objectives and areas of work for the year. Within these work areas indicators for fraud are considered. Internal Audit will also respond to requests from management and Counter Fraud Officers where there may be concerns over the effectiveness of internal controls. The work plan is agreed and monitored by the Audit Committee and Section 151 Officer.

## 8. REPORTING, ADVICE AND SUPPORT

8.1 The Council's expectation is that Members and managers will lead by example and that employees at all levels will comply with the Constitution, Council Policies, Financial Regulations, Procurement Regulations, Financial and Contract Procedure Rules, codes of conduct and directorate procedures.

8.2 The Council recognises that the primary responsibility for the prevention and detection of fraud rests with management. It is essential that employees of the Council report any irregularities, or suspected irregularities to their Line Manager and if this is not appropriate then to a Counter Fraud representative.

8.3 The Council must create the right environment so that anyone can raise concerns in respect of irregularities with the knowledge that they will be treated seriously and confidentially. The Council will provide all reasonable protection for those who raise genuine concerns in good faith, as confirmed in the Council's Whistle-Blowing Policy.

8.4 If the informant is a member of the public or external contractor, they can contact a Counter Fraud Officer at the Council to report the suspicion. This can be done anonymously. A hotline number for reporting suspicions may also be established and if so, can be found on the Council's website. The Council's complaint procedure may also be utilised but may not be the most appropriate channel.

8.5 The above process does not relate to reporting Housing Benefit Fraud allegations (which are now dealt with by the Department for Work and Pensions) or to Council Tax Reduction Scheme offences. The informant should contact the Officer nominated to deal with this; details can be found on the Council's website within the Revenues and Benefit Section information.

8.6 The Officer who receives the allegation (whether from a Member or a Council employee) must refer the matter to a Counter Fraud representative within the Council, to determine how the potential irregularity will be investigated and to whom the allegation should be discussed within the Council. This is to ensure correct investigative procedures are adhered to and that any potential fraud enquiry is not compromised.

8.7 As appropriate, reports will be issued to the Monitoring Officer, Head of Paid Service, Section 151 Officer, Senior Officers, and Cabinet Members etc. where the irregularity is material and/or could affect the reputation of the Council. Decisions will then be made with regard to the most appropriate course of action. Communications and publicity will also be managed if the matter is likely to be communicated externally.

8.8 If the investigation relates to an employee then Human Resources will be engaged and the Council's Disciplinary Procedure will also be considered however this will be managed carefully to ensure any criminal investigation is not compromised.

8.9 The Council will also work in co-operation with the following bodies (and others as appropriate) that will assist in scrutinising our systems and defences against fraud, bribery and corruption:

- Local Government and Social Care Ombudsman.
- External Audit.
- The National Fraud Initiative.
- Central Government Departments.
- HM Revenue and Customs.
- The Police.
- Trading Standards.

- The Department for Work and Pensions.
- Immigration Services.
- The Chartered Institute of Public Finance and Accountancy (CIPFA).
- The Institute of Revenues Rating and Valuation (IRRV).
- Social Housing Providers and Charitable Bodies

8.10 As detailed within this document and the Council's Whistle Blowing Policy, any concerns or suspicions reported will be treated with discretion and in confidence. Referrals can be made in confidence to the Counter Fraud and Enforcement Unit at fraud.referrals@cotswold.gov.uk who work on behalf of Cheltenham and Tewkesbury Borough Councils and Cotswold, Forest of Dean and West Oxfordshire District Councils. Concerns can also be raised via Internal Audit.

## 9. FURTHER INFORMATION

9.1 Further information on Council policy can be found in the following documents (or equivalent documentation / codes):

- The Constitution.
- Code of Conduct for Employees (or equivalent) and the Members Code of Conduct which include information in relation to gifts and hospitality and declaring and registering interests.
- Whistleblowing Policy.
- Corporate Enforcement (Prosecution) Policy.
- Proceeds of Crime and Anti-Money Laundering Policy.
- Recruitment and Selection Processes.
- RIPA / IPA Policies, Procedures and Guidance.
- Financial Rules.
- Contract Rules or equivalent.
- Fair Processing Statement.
- Disciplinary Procedure.

## 10. POLICY REVIEW

10.1. The appropriate department will review and amend this policy as necessary to ensure that it continues to remain compliant and meets legislative requirements and the vision of the Council in consultation with the Council's Chief Finance Officer, the Legal Department and Members.

10.2. Review frequency as required by legislative changes / every three years.

This page is intentionally left blank

# STROUD DISTRICT COUNCIL

# AUDIT AND STANDARDS COMMITTEE

# 16 APRIL 2024

| | | | | |
|---|---|---|---|---|
| **Report Title** | **Counter Fraud and Enforcement Unit Fraud Risk Strategy** | | | |
| **Purpose of Report** | To present the Audit and Standards Committee with a Fraud Risk Strategy, so that they may consider the approach taken by the Counter Fraud Partnership.<br>To provide assurance to the Audit Committee that the risks of fraud committed against the Council are recognised, managed and mitigated for in accordance with Council priorities, and changing fraud trends. | | | |
| **Decision(s)** | **The Committee RESOLVES to consider the Counter Fraud and Enforcement Unit Fraud Risk Strategy and associated work streams.** | | | |
| **Consultation and Feedback** | The Strategy has been shared with Governance Group which includes the Strategic Director of Resources and the Monitoring Officer. | | | |
| **Report Author** | Emma Cathcart, Head of Service,<br>Counter Fraud and Enforcement Unit<br>Email: Emma.Cathcart@cotswold.gov.uk | | | |
| **Options** | The service is a specialist criminal enforcement service working with the Gloucestershire Local Authorities, West Oxfordshire District Council and the Strategy has been introduced across the Partnership. | | | |
| **Background Papers** | None. | | | |
| **Appendices** | Appendix 1 – Fraud Risk Strategy<br>Appendix 2 – Fighting Fraud and Corruption Locally Checklist (blank)<br>Appendix 3 – Government Functional Standard – GovS 013: Counter Fraud Checklist (blank)on Policy. | | | |
| **Implications (further details at the end of report)** | Financial | Legal | Equality | Environmental |
| | Yes | Yes | Yes | No |

## 1. INTRODUCTION / BACKGROUND

1.1. Stroud District Council has joined the Counter Fraud and Enforcement Unit Partnership and as such a number of Policies and Strategies will be introduced.

1.2. Risk Management is used to identify, evaluate and manage the range of risks facing an organisation. This includes consideration relating to the risk of fraud.

1.3. Fraud is the most common crime in the UK and costs many billions of pounds to private companies, individuals and the public sector. Within Local Government this is estimated to be in the region of £2.1 billion per year. Local Authorities have a responsibility to promote and develop high standards for countering fraud and corruption in their organisations. This supports good governance and demonstrates effective financial stewardship and strong public financial management.

1.4. In administering its responsibilities, the Council has a duty to prevent fraud and corruption, whether it is attempted by someone outside or within the Council such as another organisation, a resident, an employee or Councillor.

1.5. The Council is committed to an effective counter fraud and corruption culture, by promoting high ethical standards and encouraging the prevention and detection of fraudulent activities, thus supporting corporate and community plans.

## 2. MAIN POINTS

2.1. The Counter Fraud and Enforcement Unit (CFEU) has developed a Fraud Risk Strategy for implementation across the Counter Fraud Partnership, which includes Stroud District Council. The Strategy, attached at Appendix 1, has been developed to comply with Government Functional Standards relating to counter fraud activities.

2.2. The Strategy sets out the definitions and motivations for fraud and the principles of risk management. Risk management and being 'risk aware' are vital to ensure the effective operation of the Council. The risk of fraud is ever present, and it is impossible to identify or mitigate against all risks, however by being risk aware the Council is in a better position to avoid threats, develop processes that reduce the loss or impact, and increase its ability to recover.

2.3. The Strategy identifies the high-risk areas that Local Government is susceptible to, both internally and externally. It also details the types of response methods and refers to the specific fraud response recommended for Local Government. These principles underpin the Council's plan.

2.4. As set out within the Strategy, the CFEU work with Internal Audit to provide resilience and resource in prevention, detection, response and review of detected fraud and fraud risks.

2.5. Annexed to the Strategy, and attached to this report as Appendix 2 and 3, are the Fighting Fraud and Corruption Locally Checklist and the Government Functional Standard GovS 013 Checklist. These set out best practice recommendations. The CFEU will complete these in consultation with Internal Audit to inform areas for improvement or for inclusion on the work plan.

2.6. In addition to the completion of the checklists, the CFEU will implement a series of service area reviews, with the Strategic Director of Resources approval, to identify specific fraud risks within each Council service area or department. This will include considering national and local emerging fraud risks, good practice in processes and procedure, and possible areas of risk mitigation.

2.7. A Service Specific Risk Register will then be developed with overall risks score that can be assessed, monitored and reviewed. This element of the CFEU annual work plan will be developed according to priority – high risk service areas will be addressed first.

2.8. The CFEU have reviewed the Home Office Serious and Organised Crime Local Government Checklist and has worked to raise awareness relating to the risks posed by Serious and Organised Crime. It is therefore proposed that the service specific Serious and Organised Crime risks will be transferred to the relevant service or departmental risk registers and the overarching principles will be considered within the Fraud Risk Strategy.

## 3. CONCLUSION

3.1 The Counter Fraud and Enforcement Unit Fraud Risk Strategy is the first part of the partnership fraud risk work stream.

## 4. IMPLICATIONS

### 4.1 Financial Implications

4.1.1 The strategy itself does not have any direct financial implications as a result of this report. However, the implementation of the work streams associated with the Fraud Risk Strategy will help identify loss avoidance measures and any costs associated with implementation will be contained within existing budgets.

Andrew Cummings, Strategic Director of Resources
Email: andrew.cummings@stroud.gov.uk

### 4.2 Legal Implications

4.2.1 The Fraud Risk Strategy aids the application of an effective fraud risk management regime and assists the Council in effective financial governance which is less susceptible to legal challenge.

One Legal
Email: legalservices@onelegal.org.uk

### 4.3 Equality Implications

4.3.1 The promotion of effective counter fraud controls and a zero-tolerance approach to internal misconduct promotes a positive work environment.

### 4.4 Environmental Implications

4.4.1 There are no significant implications within this category.

This page is intentionally left blank

2022

# Fraud Risk Strategy

## FRAUD RISK STRATEGY

COUNTER FRAUD AND ENFORCEMENT UNIT

**Working in partnership with Councils and organisations across Gloucestershire and West Oxfordshire to prevent fraud and loss**

# Table of Contents

# Introduction

Fraud is now the most common crime in the UK and costs many billions of pounds every year to private companies, individuals and to the public purse. The impact of fraud and related offences can be devastating. Impact ranges from unaffordable personal losses, suffered by vulnerable victims, to the ability of organisations to stay in business.

Although fraud is not an issue that any organisation wants to deal with, or possibly admit to, the reality is that most organisations will experience fraud to one degree or another; within Local Government it is widespread and pervasive. Surveys worldwide relating to fraud have found that the government and public administration sector was the second most represented sector, after banking and financial services within the private sector.

The Government estimates that fraud costs the public sector between £31bn and £53bn per year. Fraud in Local Government is estimated to account for around £2.1bn of this sum per year; this is money that could be better spent on the provision of services. The Councils and Publica, which make up the Counter Fraud and Enforcement Unit Partnership, have a duty to ensure they protect public money from the risk of fraud and whilst it is impossible to eliminate all fraud, must have a sufficiently robust control framework in place to reduce these risks.

Local Authorities have a responsibility to promote and develop high standards for countering fraud and corruption in their organisations. This supports good governance and demonstrates effective financial stewardship and strong public financial management. Local Authorities face significant challenges in relation to fraud mitigation whilst providing front line services and protecting large vulnerable groups with ever decreasing resources and income streams.

In compliance with the *Government Functional Standard GovS013: Counter Fraud* this strategy sets the direction and desired outcomes for the partnership.

An important part of this approach is the anti-fraud culture and practices which are adopted to advise and guide members and staff on the approach to the serious issues of fraud and corruption. This document provides an overview of our policy in this matter and links to the Counter Fraud and Enforcement Unit response which works to prevent, detect and deter fraud and corruption.

# FRAUD RISK STRATEGY

## Key Definitions

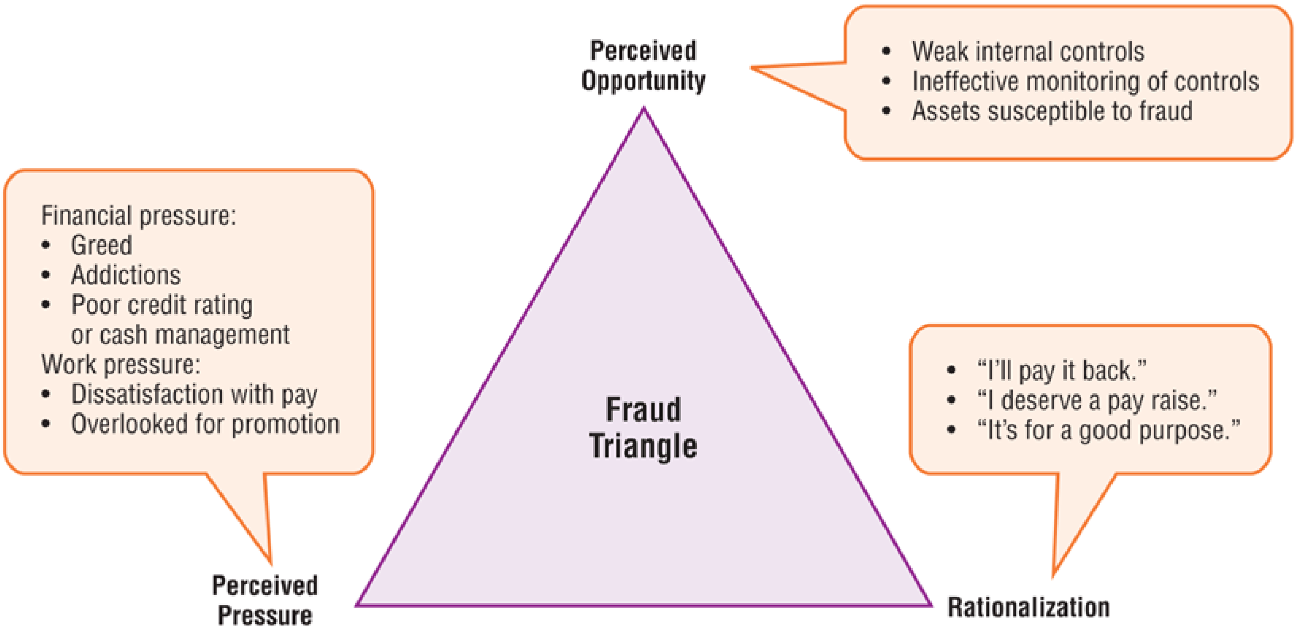
**Bribery** Bribery is defined as offering, promising, agreeing to receive or giving of a financial or other advantage to induce or reward improper functions or activities and/or the request or receipt of such an advantage.

**Corruption** For the purposes of this document, corruption in the public sector including Central and Local Government can be defined as the abuse of power by an official (or any employee entrusted to carry out the functions of government, including contractors) for personal gain.

**Fraud** The term 'Fraud' is used to define offences contrary to the Fraud Act 2006 based on false representation, dishonesty, financial gain or loss and associated offences, which include bribery and money laundering. Fraud essentially involves using deception to dishonestly make a personal gain for oneself and/or create a loss for another.

## Why do people commit fraud?

The appeal of fraud is the perceived 'low risk / high reward' opportunities it presents. The offence can be committed with relative ease and at a distance from the victim and the authorities. Within the public sector, the lack of an identifiable victim only aids the fraudster further. Fraud may also be committed by serious organised crime groups who are capable of orchestrating large scale fraud across international boundaries, but also by otherwise law abiding individuals looking to make an opportunistic gain.


Perceived Opportunity
• Weak internal controls
• Ineffective monitoring of controls
• Assets susceptible to fraud
Financial pressure:
• Greed
• Addictions
• Poor credit rating or cash management
Work pressure:
• Dissatisfaction with pay
• Overlooked for promotion
Fraud Triangle
• "I'll pay it back."
• "I deserve a pay raise."
• "It's for a good purpose."
Perceived Pressure
Rationalization

The fraud triangle is the framework commonly used to explain the reason behind an individual's decision to commit fraud. This outlines three components that contribute to increasing the risk of fraud – opportunity, incentive and rationalization. These apply equally to any sector organisation and can form part of the risk management approach but there should be recognition that the opportunities and the incentives to commit fraud are wide ranging within Local Government.

## Pressure/Motivation

In simple terms, motivation is typically based on either greed or need. Other causes cited include problems and pressures caused by debts and gambling. Many people are faced with the opportunity to commit fraud, and only a minority of the greedy and needy do so. Personality and temperament, including how frightened people are about the consequences of taking risks, play a role. Some people with good objective principles can be influenced or coerced by others or develop unaffordable habits, which tempts them to fraudulent activities. Others are tempted only when faced with financial ruin.

## Opportunity

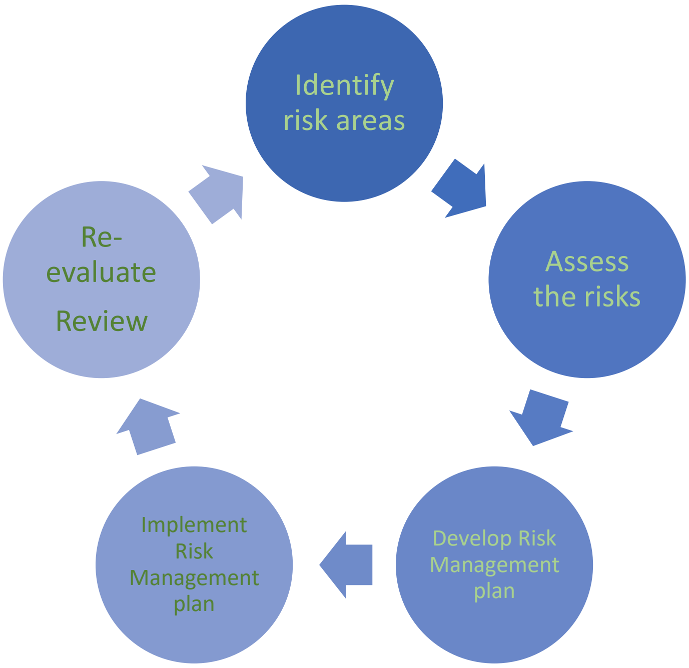
In terms of opportunity, fraud is more likely in organisations where there is a weak internal control system, poor security, little fear of exposure and likelihood of detection, or unclear policies with regard to acceptable behaviour. Research has shown that some employees are totally honest, some are totally dishonest, but that many are swayed by opportunity.

## Rationalisation

Many people obey the law because they believe in it and/or they are afraid of being shamed or rejected by people they care about if they are caught. However, some people may be able to rationalise fraudulent actions as:

- Necessary – especially when done for the business
- Harmless – because the victim is large enough to absorb the impact, or is a faceless organisation
- Justified – because 'the victim deserved it' or 'because I was mistreated.'

# Risk Management



Risk Management Cycle

## Identifying the risk - Local Government fraud risk areas

The threat of fraud not only comes from the general public (external) for whom Local Authorities provide and administer many different services, but also employees and contractors (internal), employed in a wide range of roles across a breadth of service areas. Tax is synonymous with Local Authorities and it is therefore unsurprising that losses to tax fraud in this area are significantly higher than from fraud in other areas. The below list details some of the types of fraud/corruption that Local Authorities are susceptible to:

### External High-Risk Areas

- Social Housing Tenancy Fraud (false applications, sub-letting for profit, right to buy fraud, abandonment, allocations)
- Council Tax Fraud (Discounts & Exemptions i.e. Council Tax Reduction Scheme (CTRS), Single persons discount)
- Business Rates (NNDR) Fraud (Fraudulent applications for exemptions & relief)
- Procurement, Purchasing and Contract Management Fraud (constantly changing environment and fraud can occur at any point throughout the cycle)

- Adult Social Care (care workers claiming money for time they have not worked, payments not being used to pay for care)
- Identity Fraud
- Blue Badge Scheme Abuse
- Grant Fraud
- Cyber Crime - Phishing Emails, Viruses, Payment Fraud (managed by ICT)
- Serious and Organised Crime (Licensing, contracts, Housing Right to buys, Cuckooing, online payment/payment card fraud)

### Internal Fraud Risks

- Payroll Fraud
- Fraudulent claims for expenses and allowances
- Bribery, Corruption and Abuse of Position
- Failure to declare conflicts of interest
- Pre-employment fraud – provision of false information
- Misallocation of social housing to friends/family
- Procurement Fraud
- Theft
- Manipulation of Benefits systems, Grants or Council Tax accounts for personal gain
- Asset Misappropriation
- Misuse/Manipulation of Systems

Understandably, 'external' fraud poses a much greater risk to Local Authorities with Business Rates fraud identified as the largest growing fraud type in recent years. Other areas perceived to be of the greatest fraud risk to Local Authorities are in Procurement, Council Tax (CTax) 'Single Occupancy Discount' and adult social care (CIPFA – The Local Government Counter Fraud and Corruption Strategy).

## Understanding and assessing the risk

Once risks have been identified, an assessment of possible impact and corresponding likelihood of occurrence should be made using consistent parameters that will enable the development of a prioritised risk analysis. The assessment of the impact of the risk should not simply take account of the financial impact but should also consider the organisation's viability and reputation, and recognise the political sensitivities involved.

| | | | | | | |
|---|---|---|---|---|---|---|
| LIKELIHOOD (B) | Almost Certain / Very Likely<br>5 | 5 | 10 | 15 | 20 | 25 |
| | Likely<br>4 | 4 | 8 | 12 | 16 | 20 |
| | Possible / Feasible<br>3 | 3 | 6 | 9 | 12 | 15 |
| | Unlikely / Slight<br>2 | 2 | 4 | 6 | 8 | 10 |
| | Rare / Very Unlikely<br>1 | 1 | 2 | 3 | 4 | 5 |
| | | Negligible / Insignificant<br>1 | Minor<br>2 | Moderate / Significant<br>3 | Major<br>4 | Critical<br>5 |
| | IMPACT RISKS (A) | | | | | |

## Risk Response Strategy

Strategies for responding to risk generally fall into one of the following categories:

- Risk Retention (e.g. choosing to accept small risks).
- Risk Avoidance (e.g. stopping use of certain products to avoid the risk to occurring).
- Risk Reduction (e.g. through implementing controls and procedures).
- Risk Transfer (e.g. contractual transfer of risk; transferring risks to insurers).

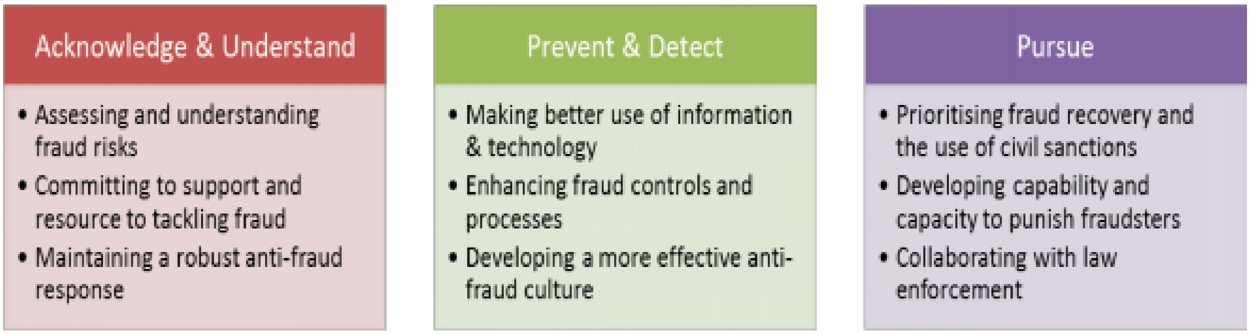
There is good assurance that the Partnership has an appropriate control framework in place to mitigate the risk of fraud. It is impossible to eliminate the risk completely and there are areas where continuous monitoring is required.

# Anti-Fraud Strategy

## Approach

The changing context in which Local Government services are delivered, the increasing risk of fraud by motivated offenders, reduced Local Authority resources and associated changes to existing local control frameworks together create a pressing need for a new approach to tackling fraud perpetrated against Local Government. Given the substantial financial losses to Local Authorities it was imperative a plan was put in place to combat fraud. In 2011, the first counter fraud strategy for Local Authorities was produced in the form of the 'Fighting Fraud and Corruption Locally' strategy (FFCL). The strategy was based on the following three principles:

- **Acknowledge** – Acknowledge and understand fraud risk.
- **Prevent** – Prevent and detect more fraud.
- **Pursue** – More robust in punishing fraud and the recovery of losses.



Acknowledge & Understand

- Assessing and understanding fraud risks
- Committing to support and resource to tackling fraud
- Maintaining a robust anti-fraud response

Prevent & Detect

- Making better use of information & technology
- Enhancing fraud controls and processes
- Developing a more effective anti-fraud culture

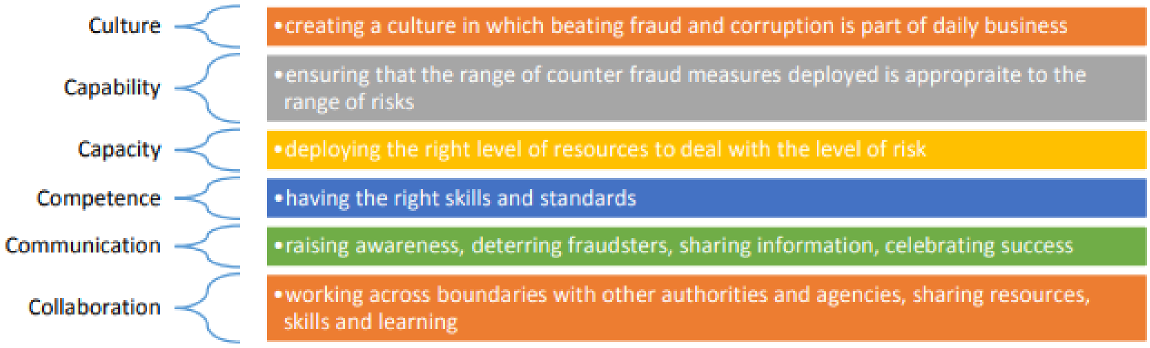
Pursue

- Prioritising fraud recovery and the use of civil sanctions
- Developing capability and capacity to punish fraudsters
- Collaborating with law enforcement

More recently a further two principles have been introduced:

- **Govern** – Setting the tone from the top and ensuring robust arrangements to ensure counter fraud and anti-corruption activities are embedded within the organisation.
- **Protect** – Protecting against serious and organised crime, protecting individuals from becoming victims and protecting against the harm fraud can do to the community. For Local Government, this includes protecting public funds, protecting the Local Authority against fraud and cyber-crime and itself from future frauds.

These principles are underpinned by the following:



| | |
|---|---|
| Culture | creating a culture in which beating fraud and corruption is part of daily business |
| Capability | ensuring that the range of counter fraud measures deployed is appropraite to the range of risks |
| Capacity | deploying the right level of resources to deal with the level of risk |
| Competence | having the right skills and standards |
| Communication | raising awareness, deterring fraudsters, sharing information, celebrating success |
| Collaboration | working across boundaries with other authorities and agencies, sharing resources, skills and learning |

The strategy was a collaborative effort between Local Authorities and key stakeholders from across the fraud arena and was designed to assist Local Authorities understand their fraud risk, assist in developing and maintaining a culture in which fraud and corruption are understood to be unacceptable, and to provide a blueprint for a tougher response (CIPFA – The Local Government Counter Fraud and Corruption Strategy).

The framework for the Council's fraud and corruption control plan includes:

- Planning and resourcing
- Prevention
- Detection
- Response

The strategy has been designed to recognise the evolving and changing risks within the public sector. Unexpected events alter the service delivery landscape and also the type and level of associated fraud risks to both public sector finances and structures. For example, the Covid-19 pandemic led Local Authorities to implement wide scale home and remote working practices swiftly. For many these service delivery changes will be permanent and the associated risks relating to cyber security or staff work integrity must be addressed. Other risks identified during the pandemic – such as the increased requirement for urgent decision making and the financial risks associated with the Business Grant payments for example – may be time limited, but can still influence and inform ongoing systems and procedures meaning there is a continued need to ensure internal controls remain effective.

## Planning and Resourcing

The Counter Fraud and Enforcement Unit (CFEU) is a corporate resource with annual work plans designed to promote awareness and deploy resource according to identified areas of weakness.

This also allows the department to provide capacity for proactive and reactive investigations in the areas that have been highlighted as high-risk.

Service specific fraud risk reviews are to be completed and reviewed annually to help identify new and emerging risks and high risk areas that require more resource.  This in turn informs the CFEU annual work plans, which together comprise the CFEU fraud response plan.

The levels of fraud, statistics and reliable information available informs risk management approaches.  It can provide evidence for necessary internal controls in particular areas known to be high risk, support a change in culture and inform best practice.  The CFEU provide quarterly reports to Corporate Management and bi-annual reports direct to Audit Committees detailing work streams and outcomes.  This ensures Councillors are briefed in relation to fraud risk.  By having a dedicated team collecting and recording this data, the partnership is ensuring a well-rounded risk management approach which is working to continuously review and improve internal controls.

The CFEU works closely with Internal Audit to identify internal control weaknesses and to ensure review and implementation of any necessary follow-up action.

## Prevention

The CFEU is responsible for developing, reviewing, and updating the Counter Fraud and Anti-Corruption, Whistleblowing and Money Laundering Policies and for any procedures linked to counter fraud or criminal investigation.

The CFEU has targeted raising awareness and changing the culture of the organisations through online training and in person awareness sessions.  In basic terms, public sector staff are more concerned about the provision of frontline services to the general public and less about financial losses and fraud.  The team have worked hard to inform staff so that they have a better understanding of fraud risks and how best to mitigate them.  Significantly, though with public bodies and the large scale diverse nature of them, it is important that any awareness training is relatable to the audience or individual staff member to gain maximum benefit.

The CFEU also introduced a revised and updated Whistle-Blowing Policy to support the fraud awareness session and ensure staff were confident in referring allegations of wrong doing to the team who specialise in protecting the identity of referral sources.

Work plans are developed annually in consultation with Internal Audit to include proactive fraud drives in high risk areas, deterrent activity and the resource for reactive case investigation work.

As Local Government continues its use of outsourcing, management should ensure that the contractors employed are aware to the principles of the Whistleblowing, Money Laundering and Counter Fraud and Anti-Corruption Policies.

The partnership is committed to ensuring that there is no modern slavery or human trafficking in its supply chains or in any part of its activities.

## Detection

The CFEU provide trained and dedicated resource for departments in the following high risk areas:-

Council Tax Discounts: – Assistance with processing National Fraud Initiative data matching, specific fraud drives and reviews, sanctions and penalty application.

Council Tax Reduction Scheme: – Authorised Officers under the Council Tax Reduction Schemes (Detection of Fraud and Enforcement) (England) Regulations 2013 to investigate cases of fraud and apply criminal sanctions, and work jointly with the DWP.

National Non Domestic Rates: – Assistance with reviews on specific exemptions and reliefs, visiting high-risk properties and business types, assistance with tracing and cross-checking data.

Procurement: – Fraud drives relating to high risk areas, review of processes and paperwork to mitigate risk and improve control mechanisms; fraud awareness training for specific officers; advice on the impact of Serious and Organised Crime and how to develop controls.

Housing Allocation, Housing and Tenancy Frauds: – Regular reviews of housing waiting lists, dedicated Housing Investigation Officers, work with Registered Social Landlords / Housing Providers, Authorised Officers under the Prevention of Social Housing Fraud Act, the ability to prepare cases for both criminal and civil action.

Internal Reactive Cases: – Undertaking disciplinary investigations involving allegations of staff or member corruption, fraud or other serious misconduct.

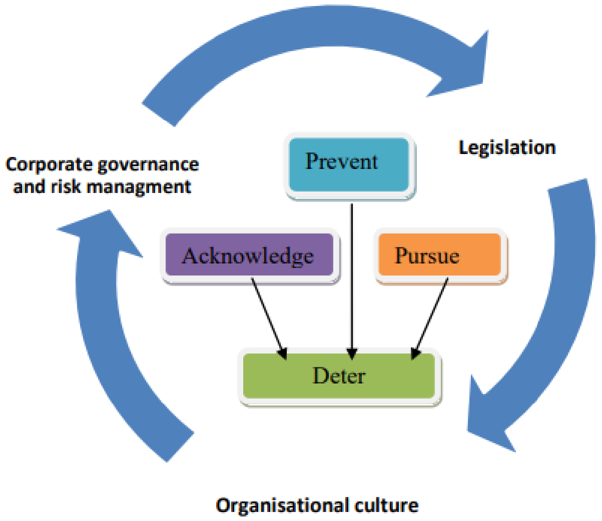
Annual Work Plans: - focussing on high risk areas nationally, or locally identified areas of risk according to the local demographic.

Fraud Risk Registers: – Development of risk registers for the Councils / Publica as a whole and for individual service areas. These are to be continually reviewed and updated.

## Response

To provide both detection and an appropriate response, the Council’s dedicated Counter Fraud and Enforcement Unit is staffed by qualified Investigation & Intelligence Support Officers with a commitment to undertaking criminal prosecutions.

# FRAUD RISK STRATEGY



The Council websites have a dedicated counter fraud page with information on how to make referrals and a summary of the work the Unit undertakes. This includes links to the relevant Policies which the individual Councils adhere to.

Internally departments can refer direct to the CFEU, and where necessary can make referrals in confidence. The CFEU works directly for the Chief Finance Officer and can liaise with any staff necessary without alerting specific individuals. In relation to sensitive whistleblowing referrals the CFEU can undertake fully confidential operations with limited notification.

The CFEU works across its partners and the wider criminal enforcement community to share good practice, develop knowledge and improve detection and prevention. Where appropriate the CFEU will refer matters to the Police or body with relevant jurisdiction.

The CFEU work to ensure that fraud awareness is maintained through regular training for staff and Members, reporting successful court cases in the media, and communicating positive outcomes with staff.

## Review

Following any proactive drive or fraud investigation, the work is subject to review and management oversight. Local Authorities have both Internal and External Audit functions and their activities, especially in key control areas, mean that they are more adaptive to the changing risk environment and are able to continuously monitor and improve any deficiencies. The CFEU and Internal Audit meet quarterly to discuss any low assurance areas and/or emerging fraud risk areas which can then be added to the work plans. Where an investigation has taken place, any areas of risk or poor control identified will be reported to the appropriate manager with recommendations for remedial action. In addition, where fraud is found during any audit work a referral is issued to the CFEU, and conversely where the CFEU has identified concerns, a report is issued to inform the Internal Audit Plan. The CFEU will also provide a report to the appropriate manager with recommendations when areas of weakness or risk are recognised, Internal Audit can also consider these recommendations and whether a follow-up Audit is required.

# FRAUD RISK STRATEGY

Policies are reviewed regularly to ensure they are relevant, in line with current good practice and legislatively up to date. Any update training this necessitates is then provided.

Service specific risk registers are reviewed regularly with the service area manager, and CFEU annual work plans are overseen by Corporate Management.

**ANNEX 1 - Fighting Fraud and Corruption Locally Checklist**

**ANNEX 2 - Government Functional Standard – GovS 013: Counter Fraud Checklist**

Agenda Item 10

Appendix 2

# Fighting Fraud and Corruption Locally (FFCL)

| What should Senior Stakeholders do? |
|---|
| The Chief Executive |
| • Ensure that your authority is measuring itself against the checklist for FFCL. |
| • Is there a trained counter fraud resource in your organisation or do you have access to one? |
| • Is the audit committee receiving regular reports on the work of those leading on fraud and is the external auditor aware of this? |
| The S.151 Officer. |
| • Is there a portfolio holder who has fraud within their remit? |
| • Is the head of internal audit or counter fraud assessing resources and capability? |
| • Do they have sufficient internal unfettered access? |
| • Do they produce a report on activity, success and future plans and are they measured on this? |
| The Monitoring Officer |
| • Are members, audit committees and portfolio leads aware of counter fraud activity and is training available to them? |
| • Is the fraud team independent of process and does it produce reports to relevant committees that are scrutinised by members? |
| The Audit Committee |
| • Should receive a report at least once a year on the counter fraud activity which includes proactive and reactive work. |
| • Should receive a report from the fraud leads on how resource is being allocated, whether it covers all areas of fraud risk and where those fraud risks are measured. |
| • Should be aware that the relevant portfolio holder is up to date and understands the activity being undertaken to counter fraud. |
| • Should support proactive counter fraud activity. |
| • Should challenge activity, be aware of what counter fraud activity can comprise and link with the various national reviews of public audit and accountability. |
| The Portfolio Lead |
| • Receives a Regular report that includes information, progress and barriers on the assessment against the FFCL checklist Fraud risk assessment and horizon scanning. |

Agenda Item 10

Appendix 2

| Checklist |
|---|
| • The local authority has made a proper assessment of its fraud and corruption risks, has an action plan to deal with them and regularly reports to its senior board and its members. |
| • The local authority has undertaken a fraud risk assessment against the risks and has also undertaken horizon scanning of future potential fraud and corruption risks. This assessment includes the understanding of the harm that fraud may do in the community. |
| • There is an annual report to the audit committee, or equivalent detailed assessment, to compare against FFCL 2020 and this checklist. |
| • The relevant portfolio holder has been briefed on the fraud risks and mitigation. |
| • The audit committee supports counter fraud work and challenges the level of activity to ensure it is appropriate in terms of fraud risk and resources. |
| • There is a counter fraud and corruption strategy applying to all aspects of the local authority's business which has been communicated throughout the local authority and acknowledged by those charged with governance. |
| • The local authority has arrangements in place that are designed to promote and ensure probity and propriety in the conduct of its business. |
| • The risks of fraud and corruption are specifically considered in the local authority's overall risk management process. |
| • Counter fraud staff are consulted to fraud-proof new policies, strategies and initiatives across departments and this is reported upon to committee. |
| • Successful cases of proven fraud/corruption are routinely publicised to raise awareness. |
| • The local authority has put in place arrangements to prevent and detect fraud and corruption and a mechanism for ensuring that this is effective and is reported to committee. |
| • The local authority has put in place arrangements for monitoring compliance with standards of conduct across the local authority covering:<br>○ codes of conduct including behaviour for counter fraud, anti-bribery and corruption.<br>○ register of interests.<br>○ register of gifts and hospitality |
| • The local authority undertakes recruitment vetting of staff prior to employment by risk assessing posts and undertaking the checks recommended in FFCL 2020 to prevent potentially dishonest employees from being appointed. |
| • Members and staff are aware of the need to make appropriate disclosures of gifts, hospitality and business. This is checked by auditors and reported to committee. |

| |
|---|
| • There is a programme of work to ensure a strong counter fraud culture across all departments and delivery agents led by counter fraud experts. |
| • There is an independent and up-to-date whistleblowing policy which is monitored for take-up and can show that suspicions have been acted upon without internal pressure. |
| • Contractors and third parties sign up to the whistleblowing policy and there is evidence of this. There should be no discrimination against whistleblowers. |
| • Fraud resources are assessed proportionately to the risk the local authority faces and are adequately resourced. |
| • There is an annual fraud plan which is agreed by committee and reflects resources mapped to risks and arrangements for reporting outcomes. This plan covers all areas of the local authority's business and includes activities undertaken by contractors and third parties or voluntary sector activities. |
| • Statistics are kept and reported by the fraud team which cover all areas of activity and outcomes. |
| • Fraud officers have unfettered access to premises and documents for the purposes of counter fraud investigation. |
| • There is a programme to publicise fraud and corruption cases internally and externally which is positive and endorsed by the council's communications team. |
| • All allegations of fraud and corruption are risk assessed. |
| • The fraud and corruption response plan covers all areas of counter fraud work: prevention, detection, investigation, sanctions and redress. |
| • The fraud response plan is linked to the audit plan and is communicated to senior management and members. |
| • Asset recovery and civil recovery are considered in all cases. |
| • There is a zero tolerance approach to fraud and corruption that is defined and monitored and which is always reported to committee. |
| • There is a programme of proactive counter fraud work which covers risks identified in assessment. |
| • The counter fraud team works jointly with other enforcement agencies and encourages a corporate approach and co-location of enforcement activity. |
| • The local authority shares data across its own departments and between other enforcement agencies. |
| • Prevention measures and projects are undertaken using data analytics where possible. |
| • The counter fraud team has registered with the Knowledge Hub so it has access to directories and other tools. |

| |
|---|
| • The counter fraud team has access to the FFCL regional network. |
| • There are professionally trained and accredited staff for counter fraud work. If auditors undertake counter fraud work they too must be trained in this area. |
| • The counter fraud team has adequate knowledge in all areas of the local authority or is trained in these areas. |
| • The counter fraud team has access (through partnership/ other local authorities/or funds to buy in) to specialist staff for surveillance, computer forensics, asset recovery and financial investigations. |
| • Weaknesses revealed by instances of proven fraud and corruption are scrutinised carefully and fed back to departments to fraud-proof systems. |

Agenda Item 10

Appendix 3

# Government functional Standard GovS 013

- Do we have an accountable individual at Member/Senior exec level who is responsible for counter fraud, bribery and corruption?
- Do we have a counter fraud, bribery and corruption strategy that is submitted to the centre?
- Do we have a fraud, bribery and corruption risk assessment that is submitted to the centre?
- Do we have a policy and response plan for dealing with potential instances of fraud, bribery and corruption?
- Do we have an annual action plan that summarises key actions to improve capability, activity and resilience in that year?
- Do we have outcome based metrics summarising what outcomes we are seeking to achieve each year? (For organisations with ‘significant investment’ in counter fraud or ‘significant estimated’ fraud loss, these will include metrics with a financial impact.
- Do we have well established and documented reporting routes for staff, contractors and members of the public to report suspicions of fraud, bribery and corruption and a mechanism for recording these referrals and allegations?
- Do we report identified loss from fraud, bribery, corruption and error, and associated recoveries, to the centre in line with the agreed government definitions?
- Do we have access to trained investigators that meet the agreed public sector skill standard?
- Do we undertake activity to try and detect fraud in high-risk areas where little or nothing is known of fraud, bribery and corruption levels, including loss measurement activity where suitable?
- Do we ensure all staff have access to and undertake fraud awareness, bribery and corruption training as appropriate to their role?
- Do we have policies and registers for gifts and hospitality and conflicts of interest?

This page is intentionally left blank

# STROUD DISTRICT COUNCIL

# AUDIT AND STANDARDS COMMITTEE

# 16 APRIL 2024

| | | | | |
|---|---|---|---|---|
| **Report Title** | **Counter Fraud and Enforcement Unit Report** | | | |
| **Purpose of Report** | To provide the Committee with assurance over the counter fraud activities of the Council.<br>Direct updates will continue to be provided biannually and are presented detailing progress and results for consideration and comment as the body charged with governance in this area.<br>The report also provides the annual update in relation to the Regulation of Investigatory Powers Act 2000 (RIPA), the Investigatory Powers Act 2016 (IPA) and the Council's existing authorisation arrangements. | | | |
| **Decision(s)** | **The Committee RESOLVES to consider and comment on the report.** | | | |
| **Consultation and Feedback** | Work plans are agreed and reviewed regularly with the Strategic Director of Resources.<br>Any Policies drafted or revised by the Counter Fraud and Enforcement Unit have been reviewed by One Legal and have been issued to the relevant Senior Officers, Governance Group and Corporate Management for comment. | | | |
| **Report Author** | Emma Cathcart, Head of Service,<br>Counter Fraud and Enforcement Unit<br>Email: Emma.Cathcart@cotswold.gov.uk | | | |
| **Options** | The Counter Fraud and Enforcement Unit is working with all Gloucestershire Local Authorities, West Oxfordshire District Council and other public sector bodies such as housing associations.<br>The Service is a shared one across the County and, as such, overheads and management costs are also shared equally meaning there is increased value for money. | | | |
| **Background Papers** | None. | | | |
| **Appendices** | None. | | | |
| **Implications (further details at the end of report)** | Financial | Legal | Equality | Environmental |
| | Yes | Yes | Yes | No |

## 1. INTRODUCTION / BACKGROUND

1.1. In administering its responsibilities, the Council has a duty to prevent fraud and corruption, whether it is attempted by someone outside or within the Council such as another organisation, a resident, an employee or a Councillor.

1.2. The Council is committed to an effective counter fraud and corruption culture, by promoting high ethical standards and encouraging the prevention and detection of fraudulent activities, thus supporting corporate priorities and community plans.

1.3. The Audit and Standards Committee oversees the Council's counter fraud arrangements, and it is therefore appropriate for the Committee to be updated in relation to counter fraud activity.

1.4. Work plans have been agreed with the Strategic Director of Resources and the Council's Management. The Audit and Standards Committee, as the body charged with governance in this area, is presented with a copy of the work plan for information.

1.5. The work plan for 2024/25 includes a focus on fraud risk mitigation regarding grant schemes and polygamous working as high-risk areas. This work will include both prevention and detection activities.

## 2. MAIN POINTS

### 2.1 Counter Fraud and Enforcement Unit Update

2.2 The CFEU Head of Service forms part of the core Multi-Agency Approach to Fraud (MAAF) group. The core group consists of attendees from Gloucestershire Constabulary Economic Crime Team, Trading Standards, Victim Support, NHS and colleagues from Gloucester City and County Councils. The MAAF has been set up to discuss fraud trends, victim care and communication of fraud scams across Gloucestershire. Through collaborative working the main purpose is to raise awareness to minimise and disrupt fraud.

2.3 It has been agreed that the Gloucestershire MAAF will have a dedicated webpage. This would be serviced through the ICT team at Tewkesbury Borough Council, funding has been requested from the Office of the Police and Crime Commissioner to support this. The website is an opportunity to put in place a communication medium that will be accessible to residents and staff in the county and beyond. This dedicated webpage will enable the group to shape fraud related messaging and offer guidance, advice on fraud and signpost people to the support that is available. The site will enable the group to educate our communities on the changing threat and to provide success stories and testimonials in order to reduce the stigma and increase reporting.

2.4 All Local Authorities participate in the Cabinet Office's National Fraud Initiative, which is a data matching exercise to help prevent and detect fraud nationwide. The use of data by the Cabinet Office in a data matching exercise is carried out with statutory authority under Part 6 of the Local Audit and Accountability Act 2014. It does not require the consent of the individuals concerned under Data Protection Legislation.

- As previously reported, earlier in the financial year, matches relating to the 2021/22 data sets resulted in increased Council Tax revenue of £142,959 and 74 Civil Penalties, totalling £5,180, being applied.
- In relation to the 2022/23 and 2023/24 data sets, the team will be confirming which matches will be the responsibility of the CFEU and the review will commence. Results will be reported in the next CFEU update report.

2.5 In addition to the strategic support and agreed annual work plan, as a dedicated investigatory support service, the CFEU undertakes a wide range of enforcement and investigation work according to the requirements of each Council. This includes criminal investigation and prosecution support for enforcement teams, investigations into staff/member fraud and corruption, or tenancy and housing fraud investigation work.

2.6 The CFEU has been tasked with undertaking the investigation of alleged fraud and abuse in relation to the Council Tax Reduction Scheme (Council Tax Support), working closely with the Department for Work and Pensions in relation to Housing Benefit investigations. Between 1 April 2023 and 21 March 2024, the team have received 20 referrals, closed 22 cases and processed enquiries for the Department for Work and Pensions. Outcomes are as reported to the Committee in January 2024.

2.7 The CFEU continues to support the Council in tackling tenancy fraud. The overall remit is to prevent, detect and deter abuse of public funds and social housing. Housing and tenancy fraud remains as one of the top four areas of fraud and abuse within the public sector. This takes many forms but the two most significant areas are Right to Buy and Illegal Subletting. The CFEU will continue to work with the Council and social housing providers to tackle this effectively.

2.8 The Counter Fraud Officers are authorised under the Prevention of Social Housing Fraud (Power to Require Information) (England) Regulations 2014. This means they are authorised to obtain information relating to an individual from organisations such as financial institutions (banks, credit card companies), utility companies, communications providers and so on. The Act also created new offences in relation to housing fraud that can be prosecuted by Local Authorities acting on behalf of Social Landlords

2.9 Between 1 April 2023 and 21 March 2024, the team have received 16 referrals and closed 14 cases. Outcomes are as reported to the Committee in January 2024.

2.10 In the same period, the team received a further 14 referrals from teams across the Council and closed 4 cases, outcomes are as reported to Committee in January 2024. Additionally, the team received 2 referrals relating to disciplinary matters, these are ongoing.

2.11 **Regulation of Investigatory Powers Act 2000 (RIPA) / Investigatory Powers Act 2016 (IPA)**

2.12 The Council's policies are based on the legislative requirements of these Acts and supporting guidance relating to directed surveillance and the acquisition of communications data.

2.13 The Polices were reviewed and presented to the Audit and Standards Committee in April 2021. The Use of the Internet and Social Media in Investigations and Enforcement Policy, was presented to Audit and Standards Committee in July 2022.

2.14 The Policies were to be reviewed within the CFEU work plan during 2023/24 and this was undertaken by the Investigatory Powers Commissioner's Office (IPCO). The Policies were fully endorsed with a request to remove any reference to the OSC Procedures and Guidance document as it has been removed from circulation. This has been done. It is not therefore proposed that the Policies will be presented to Members for approval following the review, but copies can be found on the Council's website. There have been no subsequent amendments to date.

2.15 The Council must have a Senior Responsible Officer and Authorising Officers to approve any applications for surveillance or the use of a Covert Human Intelligence Source, before the Court is approached. The Senior Responsible Officer is the Corporate Director (Monitoring Officer), Claire Hughes and the Authorising Officers are the Strategic Director of Place, Brendan Cleere and the Head of Environmental Health, Sarah Clark.

2.16 All applications for communications data are made online via the National Anti-Fraud Network (NAFN) which acts as the single point of contact for Councils. There is a requirement for the Council to nominate a Designated Senior Officer who will confirm to NAFN that the Council is aware of any request and approves its submission. This role is undertaken by the Counter Fraud and Enforcement Unit.

2.17 The Investigatory Powers Commissioner's Office and the Office for Communications Data Authorisations are the overseeing bodies of this activity. The two organisations are merging to improve efficiency whilst protecting the independent decision making of each. The merged organisation will remain under the name IPCO.

2.18 The Investigatory Powers (Amendment) Bill looks to make changes to the IPA following a review of the original Act in light of technological changes and evolving threats. A summary of any changes that impact the Council's activities will be provided as the matter progresses.

2.19 In May 2023, the Council was notified of an inspection by IPCO, regarding its compliance with the legislation. The last inspection took place in January 2022. The inspection was completed by the CFEU remotely and the report confirmed full compliance. The next inspection is due in 2026.

2.20 The CFEU has developed a summary and guidance document for all enforcement staff, this will be issued with a reminder to book refresher training with the CFEU. A copy will be issued to all Members for information and reference.

2.21 There have been no RIPA applications made by the Council during 2023/24 and no applications were made for communications data. There have been no Non-RIPA applications either.

2.22 The Council takes responsibility for ensuring its procedures relating to surveillance and the acquisition of communications data are continuously improved and all activity is recorded.

## 3. CONCLUSION

3.1 The Council is required to proactively tackle fraudulent activity in relation to the abuse of public funds. Failure to undertake such activity would accordingly not be compliant and expose the authority to greater risk of fraud and/or corruption.

3.2 If the Council does not have effective counter fraud and corruption controls, it risks both assets and reputation.

3.3 The RIPA and IPA Policies demonstrate the Council's consideration of necessity, proportionality and public interest when deciding on surveillance activity or the decision to obtain personal communication data. The application of the Policies and Procedures, to govern surveillance and the obtaining of personal communications data, minimises the risk that an individual's human rights will be breached. Furthermore, it protects the Council from allegations of the same.

## 4. IMPLICATIONS

### 4.1 Financial Implications

4.1.1 The report details financial savings generated by the CFEU and the objectives in reducing crime and financial loss to the Council. Council Tax revenue, penalty value and loss avoidance details were provided to the Committee in January 2024.

Andrew Cummings, Strategic Director of Resources
Email: andrew.cummings@stroud.gov.uk

### 4.2 Legal Implications

4.2.1 In general terms, the existence and application of an effective fraud risk management regime assists the Council in effective financial governance which is less susceptible to legal challenge.

4.2.2 The Authority is also required to ensure that it complies with the Regulation of Investigatory Powers Act 2000, the Investigatory Powers Act 2016 and any other relevant/statutory legislation regarding investigations. Any authorisations for directed/covert surveillance or the acquisition of communications data undertaken should be recorded appropriately in the Central Register.

One Legal
Email: legalservices@onelegal.org.uk

### 4.3 Equality Implications

4.3.1 The promotion of effective counter fraud controls and a zero-tolerance approach to internal misconduct promotes a positive work environment. The CFEU seeks to ensure that public authorities' actions are consistent with the Human Rights Act 1998 (HRA). It balances safeguarding the rights of the individual against the needs of society as a whole to be protected from crime and other public safety risks.

### 4.4 Environmental Implications

4.4.1 There are no significant implications within this category.

# STROUD DISTRICT COUNCIL

# AUDIT AND STANDARDS COMMITTEE

# 16 APRIL 2024

| **Report Title** | **3rd Quarter Treasury Management Activity Report 2023/24** | | | |
|---|---|---|---|---|
| **Purpose of Report** | To provide an update on treasury management activity as at 31/12/2023. | | | |
| **Decision(s)** | **The Audit and Standards Committee ACCEPTS the treasury management activity third quarter report for 2023/2024.** | | | |
| **Consultation and Feedback** | Link Asset Services (LAS). | | | |
| **Report Author** | Maxine Bell, Snr Accounting Officer<br>Tel: 01453 754134<br>E-mail: maxine.bell@stroud.gov.uk | | | |
| **Options** | None | | | |
| **Background Papers** | None | | | |
| **Appendices** | A – Prudential Indicators as of 31 December 2023<br>B – Explanation of prudential indicators | | | |
| **Implications (Further details at the end of the report)** | Financial | Legal | Equality | Environmental |
| | No | No | No | No |

## Background

1. Treasury management defined as: ‘The management of the local authority’s investments and cash flows, its banking, money market and capital market transactions; the effective control of the risks associated with those activities; and the pursuit of optimum performance consistent with those risks.’

2. This report is presented to the Audit and Standards Committee to provide an overview of the investment activity and performance for the third quarter of the financial year, and to report on prudential indicators and compliance with treasury limits.

## Discussion

3. The Chartered Institute of Public Finance and Accountancy (CIPFA) issued the latest Code in December 2021, originally adopted by this Council on 21 January 2010. This third quarter report has been prepared in compliance with CIPFA’s Code of Practice, and covers the following:

   - A review of the Treasury Management Strategy Statement (TMSS) and Investment Strategy
   - A review of the Council’s investment portfolio for 2023/24
   - A review of the Council’s borrowing strategy for 2023/24
   - A review of compliance with Treasury and Prudential Limits for 2023/24.
   - Other Treasury Issues

### Treasury Management Strategy Statement and Investment Strategy update

4. The TMSS for 2023/24 was approved by Council on 16th February 2023, some 2023/24 prudential indicators were revised in the TMSS for 2024/25 approved by Council on 22nd February 2024. The Council's Investment Strategy, incorporated in the TMSS, outlines the Council's investment priorities as follows:

   1. Security of Capital

   2. Liquidity

   3. Yield

   4. Environmental, Social and Governance (ESG)

5. In 2023-24 the Council will continue to invest for the longest permitted duration with quality counterparties to maximise return without compromising security, or liquidity. In cases where two investments of similar credit rating would generate the same return the Council selected the investment with the best ESG rating. Otherwise, the length of investments was in line with LAS advice subject to the Council's 3-year upper limit. Interest rates are forecast to be cut in the Summer, so it would be good housekeeping to invest longer locking in higher rates where possible, whilst also taking advantage of short term high Local Authority rates on offer.

6. A breakdown of the Council's investment portfolio as of 31st December 2023, is shown in Table 3 of this report.

7. Current advice from Link is to invest for no more than a year with UK banks, or up to a maximum of five years with government or local government, provided they are sufficiently highly rated on Link's weekly list.

### Investment Portfolio 2023/24

8. In accordance with the Code, it is the Council's priority to ensure security and liquidity of investments, and once satisfied with security and liquidity, to obtain a good level of return. The investment portfolio yield for the third quarter as shown in Table 1 below.

9. As set out in the Council's 2023-24 Strategy specified investments are to be benchmarked against the SONIA (Sterling Overnight Index Average) compounded 7-day and 3-month rates, see Table 4. The Council's multi-assets will be benchmarked against the 0 – 35% shares index see Table 5, and the UK other balance open-ended property fund index for the property funds see Table 6.

**TABLE 1: Average Interest Rate**

| | Period | Investment Interest Earned £ | Average Investment £m | Rate of Return |
|---|---|---|---|---|
| **Internally Managed Specified** | 01/04/2023 - 31/12/2023 | 1,788,284 | 48.203 | 4.908% |
| **Property Fund / Multi-Asset Fund** | | 242,726 | 10.000 | 3.220% |
| **Total Quarter 3** | | **2,031,011** | **58.203** | **4.632%** |

**TABLE 2: Funds Performance – Quarter 3 2023-24**

| Fund | Initial Investment<br>£m | Value as at<br>31/12/23<br>£m | Return<br>Apr - Dec<br>2023 |
|---|---|---|---|
| Lothbury | 4.000 | 3.089 | 2.98% |
| Hermes | 2.000 | 1.808 | 3.35% |
| **TOTAL PROPERTY FUNDS** | **6.000** | **4.897** | **3.10%** |
| Royal London | 3.000 | 2.811 | 3.37% |
| CCLA | 1.000 | 1.004 | 3.50% |
| **TOTAL MULTI-ASSET FUNDS** | **4.000** | **3.815** | **3.40%** |
| **TOTAL FUND INVESTMENTS** | **10.000** | **8.712** | **3.222%** |

10. As has been previously reported, we have been notified that the Lothbury property fund will be terminating. It can now be reported that this will happen on or by 30 June 2024. This means that any loss in investment value will be realised in the 2024/25 financial year. An Investment Risk earmarked reserve is held to alleviate the revenue impact of losses in investment value, which has been funded from past investment income. The amount held in this reserve will be reviewed as part of the closedown of the 2023/24 financial year.

11. The approved limits as set out in the Treasury Management Strategy report to Council 16th February 2023 within the Annual Investment Strategy were not breached during the first 9 months of 2023/24, except for Barclays which breached the limit through the re-investment of interest. In accordance with the account, after giving Barclays 95 days' notice the breach was resolved in September 2023.

12. Funds were available for investment on a temporary basis. The level of funds available was dependent on the timing of precept payments, receipt of grants and progress on the Capital Programme. The authority holds £15m core cash balances for investment purposes (i.e., funds that potentially could be invested for more than one year). The Council has invested £10m into Property and Multi-Asset Funds with the objective of longer-term investments improving the overall rate of return in future years.

13. Table 3 below shows the investments and borrowing position at the end of December 2023.

## TABLE 3: Investments & Borrowing

| | Dec 2023 | £'000 | ESG<br>Dec 23 |
|---|---|---|---|
| Aberdeen | - | | A |
| Goldman Sachs | 615 | | A |
| Deutsche | 1 | | A |
| Federated Prime | 3,519 | | A |
| **Money Market Funds Total** | | **4,135** | |
| Lloyds | 4,574 | | A- |
| **Lloyds Banking Group Total** | | **4,574** | |
| | | | |
| NatWest | 2,405 | | A- |
| **RBS Banking Group Total** | | **2,405** | |
| | | | |
| Standard Chartered | 3,600 | | BBB+ |
| Santander | 7,999 | | BBB |
| Barclays Bank Plc | 93 | | BBB+ |
| Svenska Handelsbanken | 7,037 | | A+ |
| Toronto Dominion | 4,000 | | BBB+ |
| National Bank of Canada | 2,000 | | A+ |
| Goldman Sachs International | 4,000 | | |
| **Other Banks Total** | | **28,729** | |
| | | | |
| Cheltenham Borough | 3,000 | | |
| Central Bedfordshire | 4,000 | | |
| Salford City | 3,000 | | |
| Leeds City | 2,000 | | |
| **Local Authorities** | | **12,000** | |
| | | | |
| **TOTAL INVESTMENTS** | | **£51,843** | A |
| | | | |
| Lothbury | 4,000 | | |
| Hermes | 2,000 | | |
| **TOTAL PROPERTY FUNDS** | | **£6,000** | |
| | | | |
| RLAM | 3,000 | | |
| CCLA | 1,000 | | |
| **TOTAL MULTI ASSET FUNDS** | | **£4,000** | |
| | | | |
| PWLB | | 100,717 | |
| **TOTAL BORROWING** | | **£100,717** | |

**ESG Grading Scale**

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AA+ | AA | AA- | A+ | A | A- | BBB+ | BBB | BBB- | BB+ | BB | BB- | B+ | B | B- | CCC+ |
| Negligibe | | | Low | | | | Medium | | | High | | | Severe | | |

14. Tables 4, 5 and 6 below show the benchmarked Quarter by Quarter Returns on Specified Investments and Funds at the end of December 2023.

**Table 4: Quarterly Benchmark - Specified Investments**

| Quarter | Specified Investments % return | Benchmark 7 day SONIA Compounded | Benchmark 90 day SONIA Compounded |
|---|---|---|---|
| Q1 21/22 | 0.18% | | |
| Q2 21/22 | 0.18% | | |
| Q3 21/22 | 0.19% | | |
| Q4 21/22 | 0.22% | | |
| Q1 22/23 | 0.79% | 0.87% | 0.64% |
| Q2 22/23 | 1.55% | 1.51% | 1.19% |
| Q3 22/23 | 2.66% | 2.70% | 2.12% |
| Q4 22/23 | 3.80% | 3.97% | 3.66% |
| Q1 23/24 | 4.48% | 4.53% | 4.29% |
| Q2 23/24 | 4.99% | 5.19% | 5.05% |
| Q3 23/24 | 5.26% | 5.19% | 5.22% |

**Table 5: Quarterly Benchmark - Multi-Asset Funds**

| Quarter | Fund Investments % return | Capital deficit / surplus % | Return including capital % | Benchmark 0-35% Shares |
|---|---|---|---|---|
| Q1 21/22 | 2.72% | | 2.72% | |
| Q2 21/22 | 2.60% | | 2.60% | |
| Q3 21/22 | 2.51% | 2.27% | 4.78% | 1.00% |
| Q4 21/22 | 1.89% | -6.69% | -4.80% | -3.74% |
| Q1 22/23 | 2.78% | -9.37% | -6.59% | -6.06% |
| Q2 22/23 | 2.74% | -6.15% | -3.41% | -3.69% |
| Q3 22/23 | 2.74% | 3.05% | 5.79% | 2.27% |
| Q4 22/23 | 2.77% | 1.79% | 4.56% | 1.62% |
| Q1 23/24 | 3.61% | -1.46% | 2.15% | -0.99% |
| Q2 23/24 | 3.46% | -0.02% | 3.44% | -0.78% |
| Q3 23/24 | 3.40% | 5.82% | 9.22% | 3.52% |

**Table 6: Quarterly Benchmark - Property Funds**

| Quarter | Fund Investments % return | Capital deficit / surplus % | Return including capital % | Benchmark 3 mth Property Fund Index (Other) |
|---|---|---|---|---|
| Q1 21/22 | 3.00% | | | |
| Q2 21/22 | 3.06% | | | |
| Q3 21/22 | 3.85% | 4.62% | 8.47% | 4.30% |
| Q4 21/22 | 2.71% | 5.11% | 7.82% | 6.70% |
| Q1 22/23 | 3.15% | 4.07% | 7.22% | 6.10% |
| Q2 22/23 | 3.01% | -5.87% | -2.86% | 4.00% |
| Q3 22/23 | 3.04% | -20.02% | -16.98% | -3.70% |
| Q4 22/23 | 3.07% | -0.95% | 2.12% | -14.00% |
| Q1 23/24 | 3.17% | -0.95% | 2.22% | -0.20% |
| Q2 23/24 | 3.18% | -1.92% | 1.26% | 1.30% |
| Q3 23/24 | 3.10% | -4.17% | -1.07% | -0.60% |

**External Borrowing**

15. The Council’s Capital Financing Requirements (CFR) for 2023/24 is £123,811m. The CFR denotes the Council’s underlying need to borrow for capital purposes. If the CFR is positive the Council may borrow from the PWLB or the market (External Borrowing) or from internal balances on a temporary basis (Internal Borrowing). The Council has borrowing of £100.717m as of 31st December 2023.

**Compliance with Treasury and Prudential Limits**

16. It is a statutory duty for the Council to determine and keep under review the “Affordable Borrowing Limits.” Council’s approved Treasury and Prudential Indicators are outlined in the approved TMSS.

17. During the period to 31st December 2023 the Council has operated within treasury limits (subject to the technical breach noted in paragraph 11) and Prudential Indicators set out in the Council’s TMSS and with the Council's Treasury Management Practices. The Prudential and Treasury Indicators are shown in Appendix A.

**18. IMPLICATIONS**

18.1 **Financial Implications**
There are no financial implications arising from the decision. The whole report is of a financial nature.

An investment risk earmarked reserve is held to provide some cover against fluctuating investment values. This reserve has been funded from investment income, and the level of the reserve will be reviewed at the end of the financial year.

Lucy Clothier, Accountancy Manager
Email: lucy.clothier@stroud.gov.uk

## 18.2 Legal Implications

There are no significant legal implications in respect of the recommendations in this report. Compliance with the CIPFA Code of Practice for Treasury Management in the Public Services, the ODPM Local Government Investment Guidance provides assurance that investments are, and will continue to be, within its legal powers.

One Legal,
Tel: 01684 272012 Email: legalservices@onelegal.org.uk

## 18.3 Equality Implications

There are no equality implications arising from the recommendations made in this report.

## 18.4 Environmental Implications

There are no environmental implications arising from the recommendations made in this report.

This page is intentionally left blank

| Prudential Indicator | 2023/24 Indicator £'000 | Actual as at 31 Dec 2023 £'000 |
|---|---|---|
| Capital Financing Requirement (CFR) | 123,811 | 122,645 |
| Gross Borrowing | 100,717 | 100,717 |
| Authorised Limit for external debt | 139,000 | 139,000 |
| Operational Boundary for external debt | 134,000 | 134,000 |
| Principal sums invested > 365 days | 15,000 | 10,000 |
| **Maturity structure of borrowing limits** | | |
| Under 12 months | 25% | 0% |
| 12 months to 2 years | 50% | 0% |
| 2 years to 5 years | 75% | 0% |
| 5 years to 10 years | 100% | 6% |
| 10 years and above | 100% | 94% |

This page is intentionally left blank

Appendix B

## Explanation of prudential indicators

Central Government control of borrowing was ended and replaced with Prudential borrowing by the Local Government Act 2003. Prudential borrowing permitted local government organisations to borrow to fund capital spending plans provided they could demonstrate their affordability. Prudential indicators are the means to demonstrate affordability.

**Gross borrowing** – compares estimated gross borrowing in February 2023 strategy with actual gross borrowing as at 31 December 2023.

**Capital financing requirement (CFR)** – the capital financing requirement shows the underlying need of the Council to borrow for capital purposes as determined from the balance sheet. The overall positive CFR of £123,811m provides the Council with the opportunity to borrow if appropriate. £5.693m of borrowing is planned for 2023/24 arising from the approved capital programme, together with £1.029m minimum and voluntary revenue provisions for the repayment of debt.

**Authorised limit for external debt** - this is the maximum limit for gross external indebtedness. This is the statutory limit determined under section 3(1) of the Local Government Act 2003. This limit is set to allow sufficient headroom for day to day operational management of cashflows. This limit has not been breached in the period 1 April 2023 to 31 December 2023.

**Operational boundary for external debt** – this is set as the more likely amount that may be required for day to day cashflow. This limit has not been breached in the period 1 April 2023 to 31 December 2023.

**Upper limit for fixed and variable interest rate exposure** – these limits allow the Council flexibility in its investment and borrowing options. Current investments are either fixed rate term investments or on call. Borrowing is at a fixed rate.

**Upper limit for total principal sums invested for over 365 days** – the amount it is considered can prudently be invested for a period in excess of a year. Current policy only permits lending beyond 1 year with other Local Authorities up to a maximum of 3 years. Property fund investments are subject to a 25 year maximum, and other investment funds up to 10 years as set out in Table 13 of the latest Treasury Management Strategy.

This page is intentionally left blank

# STROUD DISTRICT COUNCIL

## AUDIT AND STANDARDS COMMITTEE

## TUESDAY, 16 APRIL 2024

| | | | | |
|---|---|---|---|---|
| **Report Title** | **Draft 2024-25 Internal Audit Plan** | | | |
| **Purpose of Report** | To provide the Committee with a summary of the draft Risk Based Internal Audit Plan 2023-24, as required by the Accounts and Audit Regulations 2015 and the Public Sector Internal Audit Standards (PSIAS) 2017. | | | |
| **Decision(s)** | **The Committee RESOLVES to:**<br>**i. Note that the Draft Internal Audit Plan 2024-25 reflects the current risk profile of the Council; and**<br>**ii. Agree the Draft Internal Audit Plan 2024-25 as detailed in Appendix A.** | | | |
| **Consultation and Feedback** | Officers (Strategic Leadership Team, Heads of Service and Service Managers) and Members have been consulted on the Draft Internal Plan 2024-25.<br>Alongside Internal Audit's own assessment of risk, the consultation process is applied to ensure effective plan development in order to establish priorities and assurance requirements.<br>The timing of audit work has been planned in conjunction with the appropriate managers to minimise abortive work and time. | | | |
| **Report Author** | Piyush Fatania<br>Head of Audit Risk Assurance (ARA)<br>Tel: 01452 328883<br>Email: piyush.fatania@gloucestershire.gov.uk | | | |
| **Options** | No other options have been considered as a Risk Based Internal Audit Plan is required by the PSIAS. | | | |
| **Background Papers** | N/A – links to legislation are in the body of the report. | | | |
| **Appendices** | Appendix A – Draft Internal Audit Plan 2024-25. | | | |
| **Implications (further details at the end of the report)** | Financial | Legal | Equality | Environmental |
| | No | No | No | No |

## 1. Introduction / Background

1.1 All Councils must make proper provision for Internal Audit in line with the Accounts and Audit Regulations 2015 (the Regulations). The Regulations provide that a relevant Council 'must undertake an effective Internal Audit to evaluate the effectiveness of its risk management, control and governance processes, taking into account public sector internal auditing standards or guidance'. Completion of a risk based Internal Audit plan is based on the risk profile of the Council also supports the Section 151 Officer's duty to ensure the proper administration of the Council's financial affairs.

1.2 The guidance accompanying the Regulations recognise the PSIAS 2017 (the Standards) as representing ‘proper Internal Audit practices’. The Standards define the way in which the Internal Audit service should be established and undertake its operations. These Standards require the Head of ARA to produce a risk based Internal Audit Plan to determine the priorities of Internal Audit activity.

1.3 The proposed activity should be consistent with the Council’s priorities and objectives. It should take into account the risk management framework, risk appetite levels set by management and Internal Audit’s own judgement of risks.

1.4 To ensure Internal Audit resources continue to be focussed accordingly, it is essential that we understand the Council’s needs. This requires building relationships with key stakeholders, including other assurance and challenge providers, to gain crucial insight and ongoing understanding of the strategic and operational change agendas within the Council.

1.5 This insight is not only identified at the initial development stages of the risk based Internal Audit Plan. Dialogue continues throughout the financial year(s) and increases the ability for the Internal Audit service to adapt more closely to meet the assurance needs of the Council, particularly during periods of significant change. Our Plan is therefore dynamic and flexible to meet these needs.

## 2.0 MAIN POINTS

2.1 To ensure that an effective Plan is developed and alongside Internal Audit’s own assessment of risk, a consultation process took place with SLT, Heads of Service and Service Managers to establish priorities and assurance requirements. Audit and Standards Committee and wider Member audit requests were also considered as part of the consultation approach. The proposed activity from all sources was collated and matched against Internal Audit’s resource availability and prioritised accordingly.

2.2 The Plan is stated in terms of estimated days input to the Council of 438 audit days. By continuing to apply risk based Internal Audit planning principles, this level of input is considered acceptable to provide the Internal Audit assurance requirements of the Council.

2.3 The Head of ARA will continue to reassess Internal Audit resource requirements against the Council’s priorities and risks. As a result of this review process, the Plan will be amended throughout the year as required.

2.4 Any key changes to the Plan will be reported to the Audit and Standards Committee.

## 3.0 CONCLUSION

3.1 The PSIAS require the Head of ARA to produce a risk based Internal Audit Plan and for this Plan to be agreed by the appropriate body, which for Stroud District Council is the Audit and Standards Committee. This Audit and Standards Committee report meets the PSIAS requirement.

3.2 Regular reports on progress against the agreed Internal Audit Plan 2024-25 will be presented to the Audit and Standards Committee. These will be captured within the Audit and Standards Committee work programme for 2024-25.

## 4.0 IMPLICATIONS

### 4.1 Financial Implications

There are no financial implications arising directly from this report.

Lucy Clothier, Accountancy Manager
Email: lucy.clothier@stroud.gov.uk

Risk Assessment:
Failure to deliver effective governance will negatively impact on the achievement of the Council's objectives and priorities.

### 4.2 Legal Implications

There are no specific legal implications beyond those mentioned in the report.

Contact: One Legal
Email: legalservices@onelegal.org.uk
Tel: 01684 272691

### 4.3 Equality Implications

There are no equality implications arising from the recommendations made in this report.

### 4.4 Environmental Implications

There are no environmental implications arising from the recommendations made within this report.

This page is intentionally left blank

## Audit, Risk and Assurance - Draft Internal Audit Plan 2024-25

| Ref. | Indicative Quarter | Entity / Directorate | Activity Title | Audit Type | ARA Risk Score | Indicative Scope | Strategic Risk Register Ref |
|---|---|---|---|---|---|---|---|
| **Quarter 1** | | | | | | | |
| 1 | 1 | Resources | Payroll | Assurance | High | Completion of 2023-24 audit. | N/A |
| 2 | 1 | Communities | Business Continuity | Assurance | High | Completion of 2023-24 audit. | N/A |
| 3 | 1 | Resources | Council Tax - Opening Debit | Assurance | High | Completion of 2023-24 audit. | N/A |
| 4 | 1 | Resources | Business Rates - Opening Debit | Assurance | High | Completion of 2023-24 audit. | N/A |
| 5 | 1 | Place | Disabled Facilities Grant | Assurance | High | Completion of 2023-24 audit. | N/A |
| 6 | 1 | Communities | Out of Hours Follow-Up | Assurance | High | Completion of 2023-24 audit. | N/A |
| 7 | 1 | Communities | Section 20 Leaseholder Service Charges | Assurance | High | Completion of 2023-24 audit. | N/A |
| 8 | 1 | Resources | IT Disaster Recovery and Cyber Resilience Follow Up | Assurance | High | Completion of 2023-24 audit. | N/A |
| 9 | 1 | Resources | ICT Security Information and Event Management Process | Assurance | High | Completion of 2023-24 audit. | N/A |
| 10 | 1 | Resources | Applications Management | Assurance | High | Completion of 2023-24 audit. | N/A |
| 11 | 1 | Place | Grant certification - Sustainable Warmth Grants (Home Upgrade Grant 1 and Local Authority Delivery Scheme 3) | Grant | High | Completion of 2023-24 audit. | N/A |
| 12 | 1 | Communities | Emergency Planning | Assurance | High | To review the adequacy of the Council's Emergency Planning arrangements to ensure these are in compliance with the Civil Contingencies Act 2004. | SR4 |
| 13 | 1 | Communities | Community Hubs - including grants and food vouchers | Assurance | Medium | To assess the effectiveness of the governance, process and control arrangements over Community Hub grants, food voucher and other support activities. | SR1 and Service Risk Register |
| 14 | 1 | Communities | Homelessness Prevention | Assurance | Medium | To review whether the Council has appropriate arrangements for the prevention of homelessness to ensure compliance with legislation and regulation. | Service Risk Register |
| **Quarter 2** | | | | | | | |
| 15 | 2 | Resources | Capital Programme - Oversight and Monitoring | Assurance | High | To review the governance, risk management and monitoring arrangements in place for the Capital Programme. | SR1, SR3 and SR11 |
| 16 | 2 | Resources | ICT internal audit - Security Management Process | Assurance | High | To confirm that systems and processes in place that identify actual security incidents or potential issues and enable a timely and effective response. | SR13 |
| 17 | 2 | Resources | Medium Term Financial Plan - Future Finance Planning and Forecasting | Assurance | High | To determine the robustness of the governance structure, assumptions, and compilation process used for the development of the Council’s Medium Term Financial Plan; and forecasting against it. | SR1, SR3 and SR11 |
| 18 | 2 | Communities | Social Housing Regulation Act 2023 | Consultancy | High | To assess the Council's position against the Social Housing Regulation Act 2023 requirements; and identify opportunities for further development/consideration. | Service Risk Register |

## Audit, Risk and Assurance - Draft Internal Audit Plan 2024-25

| Ref. | Indicative Quarter | Entity / Directorate | Activity Title | Audit Type | ARA Risk Score | Indicative Scope | Strategic Risk Register Ref |
|---|---|---|---|---|---|---|---|
| 19 | 2 | Resources | Creditors | Assurance | Medium | To determine the effectiveness of the arrangement for setting up new suppliers, supplier changes and invoice control. | SR1 and Service Risk Register |
| 20 | 2 | Place | Home Upgrade Grant 2 | Grant | Medium | Grant certification requirement. Review to ensure compliance with the terms and conditions of the grant for 2023-24. Stroud lead the consortium for 7 local authorities. Total consortium funding: £6.24m. | Service Risk Register |
| 21 | 2 | Place | UK Shared Prosperity Fund | Grant | Medium | To assess the effectiveness of the governance, process and control arrangements to ensure compliance with the terms and conditions of the grant. £1.4m grant over 2022-23 to 2024-25. 2024-25 is the main year for expenditure. | SR1 and Service Risk Register |
| **Quarter 3** | | | | | | | |
| 22 | 3 | Place | Canal Project - Budget Management | Assurance | High | To review the adequacy and effectiveness of the Council's budget management arrangements for the Canal Project. | SR10 and SR18 |
| 23 | 3 | Place | Gloucestershire Building Control Partnership | Assurance | High | Option of two audits: To review the governance, risk management and monitoring arrangements in place for GBCP; or To review the governance, risk management and monitoring arrangements in place to ensure GBCP compliance with the Building Safety Act 2022 new requirements. | SR17 |
| 24 | 3 | Resources | ICT internal audit - Third Party Vendor Security | Assurance | High | For cloud hosted applications, ensure that robust contracts are in place (including clauses for ensuring effective Disaster Recovery; security standards; and the 'right to audit') that are managed and monitored effectively. | SR13 |
| 25 | 3 | Place / Resources | Section 106 | Assurance | High | To review the arrangements for Section 106 agreements, including: The recording and monitoring of agreements; Income collection and accounting procedures related to funding received; The decision-making process of using funding: and The delivery of projects. | SR1 and Service Risk Register |
| 26 | 3 | Resources | Brimscombe Port Annual Statement | Certification | Medium | Certification requirement. To verify the accuracy of the management accounts to enable certification sign-off, to conform with the funding agreement. | SR18 |
| 27 | 3 | Place | Damp and Mould - Private Sector | Assurance | Medium | To review the adequacy of the Council's arrangements for the management of damp and mould within the private sector. | Service Risk Register |

## Audit, Risk and Assurance - Draft Internal Audit Plan 2024-25

| Ref. | Indicative Quarter | Entity / Directorate | Activity Title | Audit Type | ARA Risk Score | Indicative Scope | Strategic Risk Register Ref |
|---|---|---|---|---|---|---|---|
| 28 | 3 | Place | Rural England Prosperity Fund | Grant | Medium | To assess the effectiveness of the governance, process and control arrangements to ensure compliance with the terms and conditions of the £400k grant. | SR1 |
| 29 | 3 | Resources | Contain Outbreak Management Fund | Grant | Low | Grant certification requirement. To provide assurance that, in all significant respects, the conditions of the relevant grant determination had been complied with for the period. | Service Risk Register |
| **Quarter 4** | | | | | | | |
| 30 | 4 | Place | Community Infrastructure Levy (CIL) | Assurance | High | To review the arrangements for CIL agreements, including: The recording and monitoring of agreements; Income collection and accounting procedures related to funding received; The decision-making process of using funding: and The delivery of projects. | SR1 and Service Risk Register |
| 31 | 4 | Communities | Housing - Responsive Repairs | Assurance | High | To provide assurance over the adequacy and effectiveness of Housing Responsive Repairs current controls, including the following key areas: Policies and procedures; Pre property inspections; Raising Works Orders; Variations; Completions and post completion inspections; Contractor Payments; and Tenant satisfaction. | SR1 and Service Risk Register |
| 32 | 4 | Resources | ICT internal audit - Payment Card Industry Data Security Standard (PCI DSS) | Assurance | High | To evaluate the adequacy and effectiveness of the PCI-DSS arrangements in place within the Council. To ensure that compliance is acquired and maintained in terms of policy and procedure content; in-house locations; and third parties receiving payments. Timing of audit to be flexible around PCI-DSS service actions and consultant input. | SR16 |
| 33 | 4 | Place | Climate Change - outcomes/VFM of current service delivery | Assurance | Medium | To review the oversight and monitoring arrangements for the Council's Climate Change support activities, to ensure outcomes/achievements are appropriately considered and benchmarked. Activity likely to straddle 2024-25 year end. | SR12 |
| 34 | 4 | Resources | Members Allowances and Expenses | Assurance | Medium | To review the framework of controls for administering the Members' Scheme of Allowances and evaluate the operating effectiveness of the systems and processes in place. | Service Risk Register |
| **Throughout 2024-25** | | | | | | | |
| 35 | Throughout 2024-25 | | Audit Management and Planning | Mandatory | N/A | Audit management and planning. Attendance at Committee/Board meetings. | N/A |
| 36 | Throughout 2024-25 | | Recommendation Monitoring | Mandatory | N/A | Monitoring the implementation of Internal Audit recommendations. | N/A |

## Audit, Risk and Assurance - Draft Internal Audit Plan 2024-25

| Ref. | Indicative Quarter | Entity / Directorate | Activity Title | Audit Type | ARA Risk Score | Indicative Scope | Strategic Risk Register Ref |
|---|---|---|---|---|---|---|---|
| 37 | Throughout 2024-25 | | Contingency - Assurance Work | Mandatory | N/A | Contingency to allow for the flexibility of emerging risks and due to uncertainty in time required for some audits. Contingency established to be allocated to audits that merit further allocation of time. | N/A |
| 38 | Throughout 2024-25 | | Data Analytics Support | Assurance | N/A | Time allocation to allow for data analytical support to be provided for internal audit activity throughout the year. | N/A |
| 39 | Throughout 2024-25 | | Development and implementation of new ARA Audit Management System | Project | N/A | To ensure ARA remain an efficient and effective service a new audit management system is required to be implemented in 2024-25. The existing systems licence is due to expire in 2025. System development and implementation planned to occur in 2024-25. | N/A |
| 40 | Throughout 2024-25 | Communities | Leisure - In-house Service Provision | Consultancy | High | Provision of risk and control advice as part of the future program for in-house leisure services provision. | N/A |

Q2 and Q3 have a higher workload - due to inclusion of grant/statement sign off needs (with respective deadlines) within both quarters.

# STROUD DISTRICT COUNCIL

## AUDIT AND STANDARDS COMMITTEE

## TUESDAY, 16 APRIL 2024

| | | | | |
|---|---|---|---|---|
| **Report Title** | Update on Annual Governance Statement Action Plan | | | |
| **Purpose of Report** | This report gives an update on the areas of focus identified for 2023/34 in the Annual Governance Statement 2022/23 | | | |
| **Decision(s)** | **The Committee RESOLVES to note the progress made against the Annual Governance Statement action plan** | | | |
| **Consultation and Feedback** | n/a | | | |
| **Report Author** | Claire Hughes, Corporate Director (Monitoring Officer)<br>Email: claire.hughes@stroud.gov.uk | | | |
| **Options** | None | | | |
| **Background Papers** | Annual Governance Statement 2022/23 | | | |
| **Appendices** | Appendix A – 2023/24 Action Plan | | | |
| **Implications (further details at the end of the report)** | Financial | Legal | Equality | Environmental |
| | No | No | No | No |

## 1. Introduction / Background

1.1 Regulation 6(1) of the Accounts and Audit Regulations require the publication of an Annual Governance Statement ('AGS') by the Council.

1.2 The Annual Governance Statement 2022/23 was considered and agreed by this Committee in September 2023 and was subsequently signed by the Leader and Chief Executive.

1.3 The Statement contains an action plan which sets out the actions the Council is to take in relation to the areas of focus identified within the AGS 2022/23.

1.4 This report provides the committee with the latest update against that action plan – see Appendix A.

1.5 Members are asked to note that any actions that remain outstanding at the date of this report will be carried forward into next year's action plan.

## 2. Implications

### 2.1 Financial Implications

There are no financial implications arising from this report.

Lucy Clothier, Accountancy Manager
Tel: 01453 754343 Email: lucy.clothier@stroud.gov.uk

### 2.2 Legal Implications

As detailed in the report, to evaluate good governance in practice, there is a statutory requirement under Regulation 6(1) of the Accounts and Audit England Regulations 2015 for the Council to conduct a review of the effectiveness of the system of internal control and prepare and publish an annual governance statement. The CIPFA/ Solace Delivering Good Governance in Local Government Framework defines the principles that should underpin the governance of a local authority and provides a structure to help local authorities with their approach to governance.

One Legal
Tel: 01684 272012 Email: legalservices@onelegal.org.uk

### 2.3 Equality Implications

An EIA is not required because there are not any specific changes to service delivery proposed within this decision.

### 2.4 Environmental Implications

There are no significant implications within this category.

# Annual Governance Statement– Action Plan for 2023-24

## Update April 2024

| Issue | Actions | Lead Officer | Target Date | Update |
|---|---|---|---|---|
| Update our HR and ICT Policies | Complete a review of HR and ICT policies to ensure they are fit for purpose, reflect current statutory requirements, and best practice. | Andrew Cummings | April 2024 | We have got a draft recruitment policy that is being circulated in the team for sign off and implementation by end of Jan. In addition, the following HR policies have been updated.<br>• Domestic Abuse Policy created, approved and live (training planned initially for SLT, LMT, HR, Wellbeing Ambassadors. Phase 2 training will be for unit managers and all line managers later in the summer )<br>• Probation policy reviewed, updated and live<br>• Travel and subsistence reviewed, updated and live<br>• Managing sickness absence – reviewed, updated and live<br>The HR Team is currently working on the creation of some new policies and policy edits:<br>• Carers Leave<br>• Reviewing flexible working hours in light of new legislation proposed<br>• Neonatal leave<br>HR have included a full review of HR policies in the 2024-service plan. The policies will be split across the team, based on work area, to review in terms of style language and content. |
| | Ensure that where appropriate HR and ICT policies are interconnected to ensure that appropriate procedures are in place concerning matters such as employee access to systems and data during periods of long term sickness absence or when the subject of disciplinary investigations. | Andrew Cummings | April 2024 | Completed<br>Maternity leave guidance and sick leave guidance have been reviewed, updated and rolled out and include instruction re. suspension of sensitive and confidential system access.<br>This is being updated now and will be ready by 31st March as detailed in the audit recommendation |
| | Update guidance on the use of personal devices for council business. | Owen Chandler | December 2023 | Completed |

| | | | | |
|---|---|---|---|---|
| Develop our approach to project and programme management | Establish a toolkit for projects and programmes | Hannah Barton | ~~January 2024~~ September 2024 | Ongoing – the draft toolkit has been presented to the Corporate Governance Group for feedback and will be updated before being circulated for consultation more widely. This work has been delayed until after the elections due to competing priorities. |
| | Implement a process for tracking and monitoring projects | Hannah Barton | ~~January 2024~~ September 2024 | This work has been delayed until after the elections due to competing priorities. |
| | Introduce the use of Ideagen for project management | Hannah Barton | ~~January 2024~~ September 2024 | Several projects are trialling the use of Ideagen as a project management tool and feedback will be collected before rolling this out more widely. |
| Risk Management | Complete a thorough review of the Corporate Risk Management Framework | Sarah Turner | ~~November 2023~~ February 2024 | Completed |
| | Ensure the guidance on the Hub is updated | Sarah Turner | February 2024 | Completed |
| | Provide training to officers and members | Sarah Turner | March 2024 | Officer training has been completed.<br>Member training has been scheduled to take place after the election. |
| | ARA to undertake follow up work for the Risk Management audit that was undertaken in 2022 and report progress on implementation to the ASC. | ARA | October 2023 | Completed |
| | ARA to conclude work on the production of an Assurance Map | ARA | September 2023 | Completed<br>Final report received in December 2023 |
| Complete the transition of Leisure Services | Decision to be taken on the future of leisure services by CS&L Committee, S&R Committee and Full Council by July 2023 | Ange Gillingham | July 2023 | Completed |
| | Establish governance and project management arrangements for | Ange Gillingham | September | Completed - Governance arrangements have been agreed and are now in place |

| | | | | |
|---|---|---|---|---|
| | transition to preferred model of operation | | 2023 | |
| | Complete transfer to preferred model of operation prior to expiry of contract with current provider | Ange Gillingham | October 2024 | Ongoing – this action runs over two years of the Annual Governance Statement so will be carried over into 2024/25 action plan. |
| Register of employee interests, gifts and hospitality | Introduce an annual declaration process for all staff which enables the council to hold accurate records of employee conflicts of interest, related party transactions, gifts, and hospitality | Claire Hughes | October 2023 | Completed |
| Business Continuity | Complete the review of all service business continuity plans | Claire Hughes | June 2023 | Completed |
| | Develop a corporate recovery plan | Claire Hughes | September 2023 | Completed |
| | Carry out a test of the corporate recovery plan to ensure it is fit for purpose and to learn lessons. | Claire Hughes | November 2023 | Completed |

This page is intentionally left blank

STROUD DISTRICT COUNCIL
Council Offices • Ebley Mill • Ebley Wharf • Stroud • GL5 4UB
Telephone 01453 766321 • Facsimile 01453 750932
www.stroud.gov.uk

# AUDIT & STANDARDS COMMITTEE

# OFFICER REPORT

## STRATEGIC RISK REGISTER BRIEF REPORT:

Introduction

This paper provides summary information on the key changes which have been made to the Strategic Risk Register since the last meeting of the Audit and Standards Committee

As a result of the timing of reports production there have been minimal changes to the Strategic Risk Register as Quarter 4 reporting is not yet complete. Any further changes in addition to those reported here will be verbally reported at committee.

Risks which have reviewed

**Risk SR1** has been reviewed with the risk reduced from 9 to a 6 as a result of declining probability. Inflation is still at 4% at the time of writing but the recently approved MTFP includes sufficient allowance for estimated inflation levels.

**Risk SR2** has been updated to reflect improvements in controls. No change to scoring.

**Risk SR3** has been reviewed after the recent Budget process. The risk is still regarded as having a major severity but a probability of unlikely. A balanced budget has been set for 2024/25 and is anticipated for 2025/26.

Newly added risks

**None**

Deleted Risks

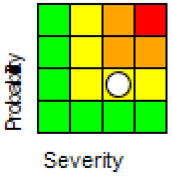
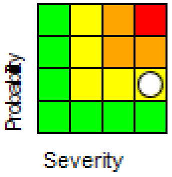
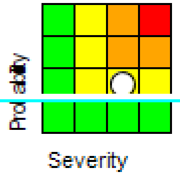
**None**

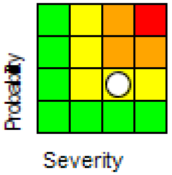
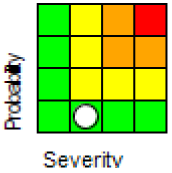
| | |
|---|---|
| **REPORT SUBMITTED BY** | Andrew Cummings |
| **DATE** | 08/04/2024 |

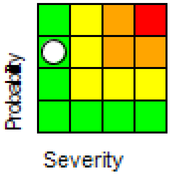
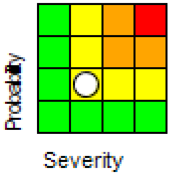
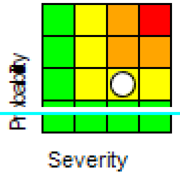
This page is intentionally left blank

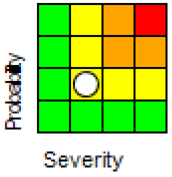
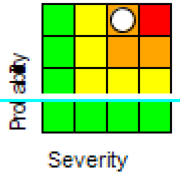
# SDC Strategic Risk Register

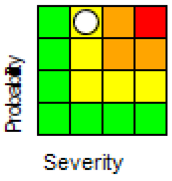
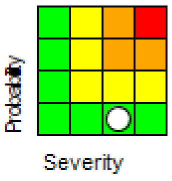
Cross cutting risks
**Generated on:** 07 April 2024

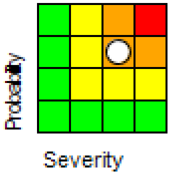
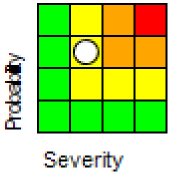
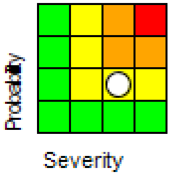
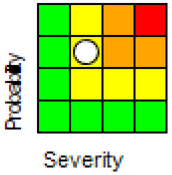
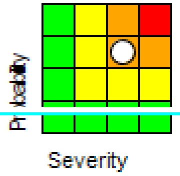
| Status | Risk Code | Title | Assigned To | Current Risk Matrix | Probability | Severity | Risk Score | Control | Control Score | Risk Target | Latest Note |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ⚠ | SR1 | High levels of inflation impacting upon Council budgets and Service Delivery | Andrew Cummings |  | 2 | 3 | 6 | The Budget Strategy and Medium Term Financial Plan should include a medium term analysis of the level of inflation. | 1 | 4 | Inflation is stable at 4% and the recent MTFP includes sufficient sums for estimated inflation levels - no impact on service delivery is anticipated. |
| | | | | | | | | Capital Budgets must include sufficient contingency to allow for inflation and this should be incorporated within the Budget Strategy. | 1 | | |
| | | | | | | | | HR Policies and Advertising should include details of the wider benefits of working for SDC | 1 | | |
| | | | | | | | | Proactive measures to reduce energy consumption | 1 | | |
| | | | | | | | | Effective procurement of energy contracts | 2 | | |
| ⚠ | SR2 | Information Governance Compliance - The loss of control of data processed by the council | Owen Chandler |  | 2 | 4 | 8 | Develop consistent Data Sharing practices and agreements | 1 | 8 | 03.24 - Automated deletion authorised. 1st phase to go live in July with additional phases impelmented based on risk/need once phase one embedded. |
| | | | | | | | | Develop Information Governance Champions | 1 | | |
| | | | | | | | | Improved insight of iGov function through improved reporting and recording of service usage, trends and feedback. | 1 | | |
| | | | | | | | | Improved retention policy compliance | 1 | | |
| | | | | | | | | Improved use of automation in council retention | 1 | | |
| | | | | | | | | Up to date and accessible Training & Guidance | 1 | | |
| ⚠ | SR3 | Failure to develop a balanced | Andrew Cummings |  | 2 | 3 | 6 | Develop a series of savings proposals and income generation opportunities to meet the targets in the MTFP | 1 | 6 | Risk remains stable after approval of MTFP. |

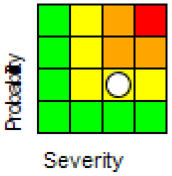
| Status | Risk Code | Title | Assigned To | Current Risk Matrix | Probability | Severity | Risk Score | Control | Control Score | Risk Target | Latest Note |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | budget managing Council Priorities within available funding | | | | | | Continue to explore the development of appropriate partnerships and efficient joint ventures | 1 | | |
| | | | | | | | | Potential to increase income through measures such as: Council Tax and fees and charges | 1 | | |
| | | | | | | | | Ensure Treasury Management and Capital Strategies are aligned with targets in the MTFP | 1 | | |
| | | | | | | | | Establish and implement a public consultation strategy | 1 | | |
| | | | | | | | | Use budget monitoring to ensure that budgetary control is maintained and income targets are monitored | 1 | | |
| ⚠ | SR4 | Emergency planning | Keith Gerrard |  | 2 | 3 | 6 | Council to identify priorities, and required resources, as part of the MTFP process | 1 | 3 | An emergency management structure is now in place and a number of key documents have been updated. |
| | | | | | | | | Ensure ICT hardware and software maintained at appropriate levels | 1 | | |
| | | | | | | | | Individual service continuity plans fit for purpose and adhered to | 1 | | |
| | | | | | | | | Workforce plan to secure expertise to avoid service failures | 1 | | |
| | | | | | | | | Ensure data backup system fit for purpose | 1 | | |
| | | | | | | | | Adequate resources on hand to respond to emergencies - To include Strategic, Tactical and Operational Response | 1 | | |
| | | | | | | | | Communication strategy to keep stakeholders informed of service availability | 1 | | |
| ✓ | SR5 | The Council is required to increase its contributions to the | Andrew Cummings |  | 1 | 2 | 2 | Ensure service redesigns or other staffing changes takes account of financial impact of changed staffing levels on pension fund contributions | 1 | 2 | |
| | | | | | | | | Ensure MTFP accurately reflects contribution | 1 | | |

| Status | Risk Code | Title | Assigned To | Current Risk Matrix | Probability | Severity | Risk Score | Control | Control Score | Risk Target | Latest Note |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Gloucestershire Pension Fund above the MTFP provision. | | | | | | likely to be required based upon current funding levels and future projections | | | |
| | | | | | | | | Ensure Treasury Management decisions take account of investment benefits potentially available from ad hoc payments to pension fund | 1 | | |
| ✓ | SR6 | Statutory changes to waste legislation could mandate waste collection alterations. | Mike Towson |  | 3 | 1 | 3 | Monitor and manage new garden waste customer requests to maximise revenue from the service. | 1 | 2 | Score downgraded following government announcements in Oct 23.  Twin streaming to be permitted and therefore no fleet change on recycling required.<br><br>Some alterations will be required in time for March 26 and March 27. |
| | | | | | | | | Effective management of UBICO contract. | 1 | | |
| | | | | | | | | Maximise effective use of existing resources. | 1 | | |
| | | | | | | | | Keeping up to date with emerging legislative changes and good practice. | 1 | | |
| △ | SR7 | Difficulty in recruiting and retaining staff with the right skills, values and behaviours | Lucy Powell |  | 2 | 2 | 4 | Adopt policies which promote staff development and retention, in line with the SDC people Strategy | 2 | 2 | Scoring changed to reflect the original position on Excelsis |
| | | | | | | | | Adoption and implementation of efficient and professional recruitment policies and practices | 2 | | |
| | | | | | | | | Purchase and implement HR software with effective recruitment modules | 2 | | |
| | | | | | | | | Where appropriate developing partnership arrangements with other public sector partners to share risk and build capacity | 1 | | |
| | | | | | | | | Transfer risk through outsourcing if appropriate | 2 | | |
| | | | | | | | | Review benefit package for staff, including financial and non-financial rewards measure | 1 | | |
| △ | SR8 | The loss of income from recycling/inc | Mike Towson |  | 2 | 3 | 6 | Effective management of UBICO contract. | 1 | 3 | No risk score change.<br><br>Recycling material markets |
| | | | | | | | | Keeping up to date with emerging legislative changes and good practice. | 2 | | |

| Status | Risk Code | Title | Assigned To | Current Risk Matrix | Probability | Severity | Risk Score | Control | Control Score | Risk Target | Latest Note |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | entive credits and the potential for increased costs of recyclate processing. | | | | | | To keep lines of communication open with the County Council to maximise the lead in time for any changes to payment received | 1 | | remain volatile, illustrated by the reduction in income from our fibre stream in 23/24.<br>Food waste incentive payments reduced in recent years, so unlikely to change further in the short term. |
| | | | | | | | | MRF Contract - the value of recylates collected by the Council are determined by industry benchmarks, this may have an impact of the amount received (income) or the costs incurred of disposal | 2 | | |
| △ | SR9 | Low of levels of staff wellbeing and mental health | Lucy Powell |  | 2 | 2 | 4 | Introduction of wellbeing champions to engage with staff across the Council to talk openly about wellbeing and working with HR, SLT and LMT to share thoughts and recommendations on staff wellbeing | 1 | 1 | Scoring changed to reflect the original position on Excelsis |
| | | | | | | | | Creation and promotion of a set of Corporate Values and Behaviours to reflect the culture that we desire at SDC | 1 | | |
| | | | | | | | | A comprehensive set of employee support tools which are also open to elected members. This is to include mental health first aiders and counselling services. | 1 | | |
| | | | | | | | | Member development group to consider development need of Councillors | 1 | | |
| | | | | | | | | Maintaining our workplace wellbeing award from Healthy Lifestyles Gloucestershire | 1 | | |
| | | | | | | | | Absence monitoring is used to track levels of mental health absences and corrective action taken where appropriate | 1 | | |
| | | | | | | | | An annual staff survey, supplemented by more regular wellbeing surveys, is used to understand the current priorities for staff and respond accordingly. | 1 | | |
| 🔴 | SR10 | Failure to deliver the canal project | Chris Mitford-Slade |  | 4 | 3 | 12 | Close monitoring at Project Team and Board level of all expenditure and forecast costs to completion | 1 | 2 | Probability risk increased to reflect delays in obtaining planning permission, the |

| Status | Risk Code | Title | Assigned To | Current Risk Matrix | Probability | Severity | Risk Score | Control | Control Score | Risk Target | Latest Note |
|---|---|---|---|---|---|---|---|---|---|---|---|
|  |  | on time and/or to budget |  |  |  |  |  | Seeking additional funding from partners and through NLHF and fund-raising, for any identified funding gaps | 1 |  | increasing funding gap and the uncertainty of the future funding streams |
|  |  |  |  |  |  |  |  | Agreeing extensions of time for project completion with NLHF and project partners as required, in light of delays caused by Covid-19, cost inflation and other external factors outside local control. | 1 |  |  |
|  |  |  |  |  |  |  |  | Continued effort to secure required consents and land (or options to secure land). | 1 |  |  |
|  |  |  |  |  |  |  |  | All project partners and NLHF kept closely informed and ready to act in the event that any of the identified triggers materialise | 1 |  |  |
| ⚠ | SR11 | Government white paper on levelling up results in changes to local government structure or funding | Andrew Cummings |  | 4 | 2 | 8 | Assess impact of White Paper and work with neighbouring authorities | 2 | 3 |  |
|  |  |  |  |  |  |  |  | Active engagement with Gloucestershire County Council as they work towards their proposal for a County Deal | 2 |  |  |
|  |  |  |  |  |  |  |  | Medium Term Financial Planning process to include financial implications of levelling as they become known | 2 |  |  |
| ✓ | SR12 | Failure of SDC to play its full part in delivering the ambitions set out in the 2030 strategy, to tackle the climate and ecological emergency and to do all in our power | Brendan Cleere |  | 1 | 3 | 3 | Monitoring to highlight areas where further/priority action needs to be taken | 1 | 1 |  |
|  |  |  |  |  |  |  |  | Effective community and partnership governance in place to drive 2030 strategy ambitions, including a community engagement board at district level and Climate Leadership Gloucestershire at county level | 1 |  |  |
|  |  |  |  |  |  |  |  | Effective co-ordination of SDC's own actions as a leader by example to tackle the climate and ecological emergency | 1 |  |  |
|  |  |  |  |  |  |  |  | Effective monitoring and public scrutiny and reporting of progress towards 2030 ambitions | 1 |  |  |

| Status | Risk Code | Title | Assigned To | Current Risk Matrix | Probability | Severity | Risk Score | Control | Control Score | Risk Target | Latest Note |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | to become a carbon neutral district by 2030 | | | | | 🟩 | | | 🟩 | |
| △🔴 | SR13 | Successful cyber attack on the Council | Adrian Blick |  | 3 | 3 | 9 | Education of SDC network users<br>Protecting SDC from penetration<br>Reducing the extent of lateral movement across the SDC IT estate should a hack occur<br>Purchase cyber insurance to partially cover costs of any successful cyber breach | 2<br>2<br>2<br>2 | 6 | No further update required |
| △ | SR14 | Business Continuity | Keith Gerrard |  | 3 | 2 | 6 | A complete review of business continuity is being undertaken.<br>Development of business continuity plans for all services<br>Creation of a comprehensive corporate recovery plan. | 1<br>1<br>2 | 3 | Severity has now reduced due to level of controls in place |
| △ | SR15 | Strike action by Ubico | Keith Gerrard |  | 2 | 3 | 6 | | | 3 | NJC Pay award has now been agreed and Ubico will be implementing for their staff.<br>The results of the anticipated second union ballot did not reach the required threshold for industrial action. |
| △ | SR16 | Non compliance with PCI DSS | Adrian Blick |  | 3 | 2 | 6 | External support being procured to enable compliance | 1 | 4 | Third Party proposal to enable gap analysis and remediation recommendations received and in review |
| △🔴 | SR17 | Failure to fulfil the requirements | Paul Bowley |  | 3 | 3 | 9 | Validation of Building Control Inspectors<br>Registration with the Building Safety Regulator | 2<br>1 | | From the 6th April 2024, legal changes associated with the building safety act 2022 will be |

| Status | Risk Code | Title | Assigned To | Current Risk Matrix | Probability | Severity | Risk Score | Control | Control Score | Risk Target | Latest Note |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | of the building safety regulator. | | | | | | Building Safety Regulator oversight | 1 | | introduced that will fundamentally change the way building control services are delivered. The building safety regulator will oversee the changes which include mandatory registration of building inspectors, operational rules and KPI's.<br>Four members of the team have sat competency exams, results are awaited. There will be one further opportunity to sit the assessment prior to the 6th April. Once validated inspectors will register with the BSR, this will determine the type of work they can assess. Validation/ registration is over a 4 year cycle.<br>Work on the OSR and KPI's has started in preparation. |
| △ | SR18 | Selected Development Partner doesn't deliver the Brimscombe Port Development resulting in delays to the delivery of new housing and the restoration of | Ali Fisk |  | 2 | 3 | 6 | Effective Dialogue with Development Partner | 1 | 3 | |

| Status | Risk Code | Title | Assigned To | Current Risk Matrix | Probability | Severity | Risk Score | Control | Control Score | Risk Target | Latest Note |
|---|---|---|---|---|---|---|---|---|---|---|---|
|  |  | the Port Basin and reputational damage to the authority |  |  |  |  | 🟨 |  |  | 🟩 |  |

| Risk Status |  |
|---|---|
| 🛑 | Alert |
| ⚠ | High Risk |
| ⚠ | Warning |
| ✅ | OK |
| ❓ | Unknown |

## STROUD DISTRICT COUNCIL

## AUDIT AND STANDARDS COMMITTEE

## 16 APRIL 2024

## WORK PROGRAMME

| Meeting Date | Report Description | Responsible Officer / Member |
|---|---|---|
| 16 July 2024 | Internal Audit Progress Report | Head of ARA |
| | Annual Governance Statement Update | Monitoring Officer |
| | Treasury Management Outturn 2023/24 | Principal Accountant |
| | External Audit Plan | Deloitte |
| | Unaudited Statement of Accounts 2023/24 | Principal Accountant |
| | Annual Report 2023/24 | Head of ARA |
| | Annual Report of the Chair | Chair |
| | Standing Items:<br>a) Corporate Risk Register Update<br>b) To consider the work programme | Strategic Director of Resources<br>Democratic Services |
| 24 September 2024 | Internal Audit Progress Report | Head of ARA |
| | Treasury Management Q1 Report | Principal Accountant |
| | Annual Report 2023/24 | Head of ARA |
| | Corporate Care Standards Performance Update | Community Access & Engagement Manager |
| | Standing Items:<br>a) Corporate Risk Register Update<br>b) To consider the work programme | Strategic Director of Resources<br>Democratic Services |
| 19 November 2024 | Internal Audit Progress Report | Head of ARA |
| | Half-Year Treasury management | Principal Accountant |
| | Annual Audit Letter | Deloitte |
| | Annual Code of Conduct Report | Monitoring Officer |
| | Contract Management Framework Update | Senior Policy and Governance Officer |
| | Standing Items:<br>a) Corporate Risk Register Update<br>b) To consider the work programme | Strategic Director of Resources<br>Democratic Services |
| 28 January 2025 | Internal Audit Progress Report | Head of ARA |
| | Half-Year Treasury management | Principal Accountant |
| | Annual Audit Letter | Deloitte |
| | Contract Management Framework Update | Senior Policy and Governance Officer |
| | Counter Fraud and Enforcement Unit Report | Head of Service, (CFEU) |
| | Annual Governance Update | Monitoring Officer |
| | Treasury Management Strategy | Principal Accountant |
| | Standing Items:<br>a) Corporate Risk Register Update<br>b) To consider the work programme | Strategic Director of Resources<br>Democratic Services |
| 1 April 2024 | Internal Audit Progress Report | Head of ARA |
| | Counter Fraud Unit Update and Annual RIPA/IPA Update | Head of Service, (CFEU) |
| | Counter Fraud and Enforcement Unit Fraud Risk Strategy | Head of Service, (CFEU) |

| | | |
|---|---|---|
| | Counter Fraud and Anti-Corruption Policy | Head of Service, (CFEU) |
| | Information Governance Framework | Information Governance Officer |
| | Draft Internal Audit Plan 2024/25 | Head of ARA |
| | Standing Items:<br>a) Corporate Risk Register Update<br>b) To consider the work programme | Strategic Director of Resources<br>Democratic Services |

# STROUD DISTRICT COUNCIL

# AUDIT AND STANDARDS COMMITTEE

# TUESDAY, 16 APRIL 2024

| | | | | |
|---|---|---|---|---|
| **Report Title** | Internal Audit Progress Update Report 2023-24 | | | |
| **Purpose of Report** | To inform Members of the Internal Audit activity progress in relation to the approved Internal Audit Plan 2023-24. | | | |
| **Decision(s)** | **The Committee resolves to:**<br>**i. Accept the progress against the Internal Audit Plan 2023-24; and**<br>**ii. Accept the assurance opinions provided in relation to the effectiveness of the Council's control environment (comprising of risk management, control and governance arrangements).** | | | |
| **Consultation and Feedback** | Internal Audit findings are discussed with Service Heads and Managers. Management responses to recommendations are included in each assignment report. | | | |
| **Report Author** | Piyush Fatania<br>Head of Audit Risk Assurance (ARA)<br>Tel: 01452 328883<br>Email: piyush.fatania@gloucestershire.gov.uk | | | |
| **Options** | There are no alternative options that are relevant to this matter. | | | |
| **Background Papers** | None. | | | |
| **Appendices** | Appendix A – Internal Audit Activity Progress Report 2023-24<br>Appendix B – Exempt | | | |
| **Implications (further details at the end of the report)** | Financial | Legal | Equality | Environmental |
| | No | No | No | No |

## 1.0 Introduction / Background

1.1 Members agreed the Stroud District Council Internal Audit Plan 2023-24 on 18th April 2023.

1.2 In accordance with the Public Sector Internal Audit Standards (PSIAS) 2017, this report details the outcomes of Internal Audit work carried out in accordance with the agreed Plan.

## 2.0 MAIN POINTS

2.1 The Internal Audit Activity Progress Report 2023-24 at **Appendix A** summarises:

i. The progress against the Internal Audit Plan 2023-24;
ii. The outcomes of the 2023-24 Internal Audit activity delivered up to mid-March 2024; and
iii. Special investigations and counter fraud activity.

2.2 The report is the third report in relation to the Internal Audit Plan 2023-24.

## 3.0 CONCLUSION

3.1 The report purpose is to inform the Committee of Internal Audit work undertaken to date, and the assurances given on the adequacy and effectiveness of the Council's control environment. Completion of the Internal Audit Activity Progress Reports ensures compliance with the PSIAS, the Council Constitution and the Audit and Standards Committee Terms of Reference.

## 4.0 IMPLICATIONS

### 4.1 Financial Implications

There are no financial implications arising directly from this report.

Lucy Clothier, Accountancy Manager
Email: lucy.clothier@stroud.gov.uk

Risk Assessment:
Failure to deliver effective governance will negatively impact on the achievement of the Council's objectives and priorities.

### 4.2 Legal Implications

Monitoring the implementation of Internal Audit recommendations assists the Council to minimise risk areas and thereby reduce the prospects of legal challenge.

Contact: One Legal
Email: legalservices@onelegal.org.uk
Tel: 01684 272691

### 4.3 Equality Implications

There are no equality implications arising from the recommendations made in this report.

### 4.4 Environmental Implications

There are no environmental implications arising from the recommendations made within this report.

STROUD DISTRICT COUNCIL

ARA
AuditRiskAssurance

Gloucester City Council STROUD DISTRICT COUNCIL Gloucestershire COUNTY COUNCIL

# PROGRESS REPORT ON INTERNAL AUDIT ACTIVITY

## APRIL 2024

Appendix A

## 1. Introduction

1.1 The Council’s Internal Audit service is provided by Audit Risk Assurance (ARA) under a Shared Service agreement between Gloucestershire County Council, Stroud District Council and Gloucester City Council.

1.2 ARA provides these services in accordance with the Public Sector Internal Audit Standards 2017 (PSIAS) which represent the “proper Internal Audit practices”. The standards define the way in which the Internal Audit service should be established and undertake its operations.

1.3 In accordance with the PSIAS, the Head of Internal Audit is required to regularly provide progress reports on Internal Audit activity to management and the Audit and Standards Committee. This report summarises:

i. The progress against the Internal Audit Plan 2023-24;

ii. The outcomes of the 2023-24 Internal Audit activity delivered up to mid-March 2024; and

iii. Special investigations and counter fraud activity.

1.4 Internal Audit plays a key role in providing independent assurance and advice to the Council that these arrangements are in place and operating effectively. However, it should be emphasised that management are responsible for establishing and maintaining appropriate risk management processes, control systems (financial and non-financial) and governance arrangements.

1.5 The following Assurance criteria are applied to Internal Audit reports:

i. Substantial assurance – all key controls are in place and working effectively with no exceptions or reservations. The Council has a low exposure to business risk;

ii. Acceptable assurance – all key controls are in place and working but there are some reservations in connection with the operational effectiveness of some key controls. The Council has a low to medium exposure to business risk;

iii. Limited assurance – not all key controls are in place or are working effectively. The Council has a medium to high exposure to business risk; and

iv. No assurance – no key controls are in place, or no key controls are working effectively. The Council has a high exposure to business risk.

## 2. Summary of 2023-24 Internal Audit work delivered up to October 2023

| Audit | Assurance Level | Supporting Paragraph |
|---|---|---|
| Liberty Create Development | Substantial | 2.1 |
| Planning Enforcement Follow-Up | Substantial | 2.2 |
| ICT Back Up Process | Acceptable | Exempt |
| Risk Management Follow-Up | N/A | 2.3 |
| Out of Hours (OOH) Follow-Up | N/A | 2.4 |

### 2.1 Audit Activity: Liberty Create Development (Service Area: Resources)

i. Assurance Level for this report: Substantial; and

ii. Recommendations arising from this review have been prioritised as:

| | |
|---|---|
| High Priority: | 0 |
| Medium Priority: | 3 |
| Low Priority: | 1 |
| Rejected: | 0 |

2.1.1 **Scope** – The procedures and controls in place for the Liberty Create Development function were reviewed.

2.1.2 Fit for the Future is the Council's main transformation programme. The Service Delivery workstream operates under the Fit for the Future Programme and is responsible for documenting and re-engineering the Council's processes. Liberty is the main development platform used within the Service Delivery workstream. It is used to integrate existing Council systems and to develop new ways of working once process re-engineering work has been completed.

2.1.3 **Key Findings**

i. There is a substantial level of governance and assurance operating over the Liberty Create Development Programme.

ii. The Fit for the Future Programme's prime objective, "Putting the Customer at the heart of everything we do", was apparent across the audit objectives and from all staff who contributed to this review.

iii. A thorough and comprehensive understanding of the Liberty Create Development function was evident and demonstrated to the Auditor during the review.

iv. The programme's collaborative approach of working through process improvements at an individual service level is delivering a breadth of benefits for both the programme and the services. For example, Building Services and Planning Services.

v. The programme has a significant amount of work in the pipeline, awaiting implementation. Officers appointed to the Service Delivery workstream are currently either seconded or working part-time on the programme. Consideration should be given to how the Liberty Create Development Programme becomes a mainstream function. This would mitigate some of the challenges, such as long-term resource planning, workstack prioritisation and dual roles, associated with being a temporary programme. This would, in turn, offer the ability to plan, scope and deliver on a long-term basis.

**Opportunity:** To build on positive momentum already being generated by the programme.

**Recommendation**: The Council should consider:

- How to transition the process re-engineering and improvements aspects from its current temporary status into a mainstream function;

- The resource requirements for the programme in the long-term. Some specifically targeted additional resources (for example a process re-engineering or development resource) may enable the programme to bring forward delivery or increase the speed of project delivery going forward; and

- How the programme’s collaborative approach with the services is further encouraged and appropriately resourced.

vi. The Service Delivery workstream is delivering clear and tangible benefits, such as enhanced customer choice, streamlined processes and efficiency savings. It is also delivering intangible improvements, such as collaborative working between the Council’s services. There is clear evidence of the programme’s documentation of the tangible efficiencies being delivered, usually following process re-engineering or data capture from the delivery of new developments.

**Opportunity**: To ensure that all relevant benefits are captured and the workstream team’s efforts are fully highlighted.

**Recommendation**: The programme team should continue their work on documenting and reporting benefits realisation but should also consider how they capture and report all relevant benefits. For example, increases in customer satisfaction and employee engagement.

## 2.2 Audit Activity: Planning Enforcement Follow-Up (Service Area: Place)

i. Assurance Level for this report: Substantial; and

ii. No recommendations arising from this review.

2.2.1 **Scope –** The original review of Planning Enforcement was reported in November 2021 and resulted in 13 recommendations. An interim follow-up review was then completed in April 2023 and confirmed the implementation of nine recommendations, with four either outstanding or in progress.

2.2.2 This report focused on the Council’s position against the four remaining audit recommendations only.

### 2.2.3 Key Findings

i. The follow-up review confirmed all four recommendations had been implemented. Relevant actions included:

- Introduction of a time and task analysis for a two-month period, to obtain timesheet and resource need data on the relationship between direct and non-direct service activities;

- Development of a service delivery resourcing assessment. The exercise considered and identified the resource need to deliver the change programme and to operate the Planning Enforcement Protocol and case referrals; and

- Submission of a business case for additional resource to meet the forecast service needs, through the Council's "Revenue Budget Setting 2024-25 to 2027-28: Budget Pressures Request" process.

ii. From reviewing the 2024-25 Planning Enforcement Revenue budget it was confirmed that it included the annual employment cost for the additional Planning Enforcement Officer. Following Council approval of the 2024-25 Revenue budget, the "authority to fill" staff recruitment process and associated documentation will be initiated for the additional post. This 2024-25 revenue budget process inclusion confirms implementation of the relevant follow-up recommendation.

iii. The ARA Follow-Up approach has been revised within 2023-24. Future follow-up internal audit activities will not be allocated an Assurance Level.

## 2.3 Audit Activity: Risk Management Follow-Up (Service Area: Resources)

2.3.1 The audit followed up the implementation of six recommendations made from the original 2021-22 audit, five of which were medium priority and one low priority.

2.3.2 The follow-up audit was timed to ensure consideration of Ideagen, the Council's performance and risk management system that was introduced in April 2023. The follow-up confirmed that five recommendations were implemented and one was in progress.

2.3.3 The implemented recommendations included:

i. Review and update of the Council's Risk Management Policy Statement Policy Strategy. Audit and Standards Committee approval of the document was obtained in April 2023. Recommendation 1 – Medium Priority.

ii. Regular review of the Strategic Risk Register by the Audit and Standards Committee. 'Corporate Risk Register Update' has been a standing item on the Audit and Standards Committee agenda from July 2022. This is supported by regular Member risk management training; and all Members having access to the Strategic Risk Register on Ideagen. Recommendation 2 – Medium Priority.

iii. Completion of a risk management survey with Leadership Management Team to support update of the Risk Management Policy Statement and Strategy; the Risk

Management Toolkit; and training for officers. Recommendation 4 – Medium Priority.

iv. The provision of ongoing risk management training for officers. The most recent training was delivered between 26th January 2024 and 20th February 2024, aligning to the Council's new Risk Management Toolkit and the Ideagen risk management process. Recommendation 5 – Medium Priority.

v. Risk Champions have been established within the Policy and Governance Team to provide support to the wider Council on risk management and Ideagen use. This approach will be reviewed within 2024-25. Recommendation 6 – Low Priority.

2.3.4 The development of a risk assurance map (Recommendation 3 – Medium Priority) was in progress at the point of audit follow-up.

2.3.5 The Risk Assurance Map consultancy review outcomes were reported to Audit and Standards Committee in January 2024. The focus of the consultancy assignment was to support the Council with the development of a risk assurance map through the provision of advice, guidance and progression options. The Council target to draft a risk assurance map by the end of quarter 1 2024-25, with presentation to the following Audit and Standards Committee meeting.

## 2.4 Audit Activity: OOH Follow-Up (Service Area: Communities)

2.4.1 The audit followed up the implementation of 24 agreed recommendations made from the original 2021-22 audit, 12 of which were high priority and 12 medium priority.

2.4.2 The follow-up audit confirmed that all 24 recommendations have been implemented. This has been actioned by the Council through:

i. In-sourcing the OOH repairs service from June 2022 with contracts in place for specific repair specialisms. The OOH call handling service is also delivered through a contract, with contract provider change in quarter 4 2022-23.

ii. Defined service roles and responsibilities. Service delivery oversight is provided by the Operations Manager and the Head of Assets and Investments.

iii. OOH service Procedures Manual updated to include all key areas (for example, roles and responsibilities, service objectives, performance management, and business continuity arrangements).

iv. OOH call handling process flowchart update for use by the OOH call handling contractor and the Council.

v. Evidenced risk management arrangements, including risk review at service and contract meetings and update of relevant Ideagen risk registers.

vi. Contract Management Framework refresh, approval and roll out to officers. For example, updated guidance on contract extension; contract failure reviews and reporting; and contract exit strategy and lessons learned.

vii. Evidenced regular performance review of the OOH call handling contract. For example, key performance indicators are scrutinised at each contract meeting between the Council and the OOH call handling contractor.

## 3.0 Counter Fraud Update – Summary of Counter Fraud Activities

### 3.1 Current Year Counter Fraud Activities

i. To date in 2023-24 there has been one new irregularity referred to the ARA Counter Fraud Team (CFT). This case has now been closed.

ii. The case was in respect of a resident who had claimed Council Tax single person discount. The Council received information advising that the individual was not living alone in the property and therefore was not eligible for the discount. The claims were investigated, and this has now been resolved and the discount removed.

iii. Not all investigations (for example conduct, non-compliance and ethics issues) can have an assessed value attached to them or result in the recovery of monies. CFT investigations, analytics and consultative work may add value in other ways such as providing assurance to members and residents, reducing Council vulnerabilities and mitigating risk.

iv. It should be noted that many of the cases referred to the CFT involve intricate detail and, sometimes, police referral. This invariably results in a delay before the investigation can be classed as closed and the summary outcome reported to Committee.

v. In addition to the above, Counter fraud advice and alerts are routinely provided outside of the creation of referrals and cases.

vi. The CFT also maintains the Council's counter fraud intranet and webpages.

### 3.2 National Fraud Initiative (NFI)

i. Internal Audit continues to support the NFI which is a biennial data matching exercise administered by the Cabinet Office. Stroud District Council data for the 2022-23 NFI exercise has been uploaded successfully and is considered compliant.

ii. Data matches have been released by NFI and are now available for the Council teams to review.

iii. The Council has signed up to participate in a couple of NFI pilot schemes. One 'Council Tax data to Deceased Data' and the other being 'Housing Tenancy'.

iv. The full NFI timetable can be found using the link available on GOV.UK – https://www.gov.uk/government/publications/national-fraud-initiative-timetables.

v. Examples of data sets includes housing, insurance, payroll, creditors, council tax, electoral register and licences for market trader/operator, taxi drivers and personal licences to supply alcohol.

vi. Not all matches are always investigated but where possible all recommended matches are reviewed by either Internal Audit or the appropriate service area within the Council.

### 3.3 National Anti-Fraud Network (NAFN)

i. NAFN is a public sector organisation which exists to support its members in protecting the public interest. It is one of the largest shared services in the country managed by, and for the benefit of its members and currently hosted by Tameside MBC.

ii. Membership is open to any organisation which has responsibility for managing public funds and/or assets. Use of NAFN services is voluntary, which ensures the provision of value for money. Currently, almost 90% of local authorities are members and there are a rapidly growing number of affiliated wider public authorities including social housing providers.

iii. Many potential attempted frauds are intercepted. This is due to a combination of local knowledge together with the credible national communications including those from the NAFN being swiftly cascaded to teams where more national targeted frauds are shared for the purpose of prevention.

Agenda Item 16

Appendix B

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank

Stroud District Council 2023-24 Internal Audit Progress Report - April 2024

| Ref | Plan Quarter | Actual Quarter | Dept. | Audit | Comment | Risk | Status Now | Status Last Report | Comments |
|---|---|---|---|---|---|---|---|---|---|
| **Completion of 2022-23 Work** | | | | | | | | | |
| 1 | C/fwd | | Communities | Leisure Facilities – Stratford Park | Assurance | High | Final Report Issued | Final Report Issued | Reported to September 2023 Committee. |
| 2 | C/fwd | | Place | Canal Restoration Project – Risk Management | Assurance | High | Final Report Issued | Final Report Issued | Reported to January 2024 Committee. |
| 3 | C/fwd | | Place | Planning Enforcement | Consultancy | Consultancy | Final Report Issued | Final Report Issued | Reported to September 2023 Committee. |
| 4 | C/fwd | | Resources | IT Applications Management | Assurance | High | Field Work Started | Field Work Started | Terms of Reference agreed by ICT management November 2023. Field work commenced |
| 5 | C/fwd | | Communities | Cleaner Estates Strategy (Refuse) | Assurance | High | Final Report Issued | Final Report Issued | Reported to September 2023 Committee. |
| 6 | C/fwd | | Communities | Leisure Facilities – The Pulse | Assurance | High | Final Report Issued | Final Report Issued | Reported to September 2023 Committee. |
| 7 | C/fwd | | Communities | Safeguarding | Assurance | High | Final Report Issued | Final Report Issued | Reported to January 2024 Committee. |
| 8 | C/fwd | | Resources | Member Expenses | Assurance | Medium | N/A | N/A | Following the annual planning and risk evaluation exercise at the start of 2023-24 this audit did not meet the threshold for inclusion in the 2023-24 plan. Error in previous Committee update that the audit was planned. |
| 9 | C/fwd | | Resources | Risk Assurance Mapping | Consultancy | Consultancy | Final Report | Final Report Issued | Reported to January 2024 Committee. |
| 10 | C/fwd | | Council Wide | Contract Management Framework | Assurance | High | Final Report Issued | Final Report Issued | Reported to January 2024 Committee. |
| 11 | C/fwd | | Council Wide | Fit for the Future Programme | Assurance | High | Final Report Issued | Final Report Issued | Reported to September 2023 Committee. |
| 12 | C/fwd | | Resources | Insurance | Assurance | High | Final Report Issued | Final Report Issued | Reported to January 2024 Committee. |
| 13 | C/fwd | | Communities | Housing Voids – Follow-Up | Assurance | High | Final Report Issued | Final Report Issued | Reported to September 2023 Committee. |
| 14 | C/fwd | | Place | Planning Enforcement – Follow-Up | Assurance | High | Final Report Issued | Field Work Started | Final report issued in January 2024. |
| 15 | C/fwd | | Place | Sustainable Warmth Grant (Home Upgrade Grant Phase 1) | Assurance | High | Final Report Issued | Final Report Issued | Reported to September 2023 Committee. Final grant certification is required later in 2023-24. |
| 16 | C/fwd | | Place | Sustainable Warmth Grant (Local Authority Delivery Scheme Phase 3) | Assurance | High | Final Report Issued | Final Report Issued | Reported to September 2023 Committee. Final grant certification is required later in 2023-24. |
| 17 | C/fwd | | Resources | Right To Buy | Assurance | High | Final Report Issued | Final Report Issued | Reported to January 2024 Committee. |
| 18 | C/fwd | | Resources | Treasury Management and Ethical Investments Strategy | Assurance | High | Final Report Issued | Final Report Issued | Reported to September 2023 Committee. |
| 19 | C/fwd | | Council Wide | Section 31 Biodiversity Net Gain Grant | Grant | High | Final Report Issued | Final Report Issued | Reported to September 2023 Committee. |
| 20 | C/fwd | | Resources | Covid 19 Business Grants–Post Payment Assurance | Assurance | High | Final Report | Final Report Issued | Reported to September 2023 Committee. |
| **Work Planned for 2023-24** | | | | | | | | | |
| 1 | 1 | 2 to 4 | Communities | Out of Hours Emergencies - Limited Assurance Follow-Up | Assurance | High | Final Report Issued | Field Work Started | Final report issued to management in March 2024. |
| 2 | 1 | 2 to 4 | Communities | Section 20 Leaseholder Service Charges | Assurance | High | Draft Report Issued | Field Work Started | Draft report issued to management in February 2024. It is intended to finalise the report in March 2024. |
| 3 | 1 | 1 | Communities | Social Housing Decarbonisation Fund Wave 1 | Assurance | High | Final Report Issued | Final Report Issued | Reported to September 2023 Committee. |

Agenda Item 16

Appendix C

**Stroud District Council 2023-24 Internal Audit Progress Report - April 2024**

| Ref | Plan Quarter | Actual Quarter | Dept. | Audit | Comment | Risk | Status Now | Status Last Report | Comments |
|---|---|---|---|---|---|---|---|---|---|
| 4 | 1 | N/A | Resources | Corporate Asset Management Strategy | Assurance | High | Deferred | Deferred | Communication with Head of Property Services completed. Updated Strategy due to be presented to February 2024 Strategy and Resources Committee for approval. Audit deferred for consideration in 2024-25 Internal Audit Plan. |
| 5 | 1 | 2 to 4 | Resources | ICT - Liberty Create | Assurance | High | Final Report Issued | Field Work Started | Final report issued in February 2024. |
| 6 | 2 | 2 to 4 | Resources | ICT Back Up Process | Assurance | High | Final Report Issued | Draft Report Issued | Final report issued in January 2024. |
| 7 | 2 | 3 to 4 | Resources | Payroll Administration | Assurance | High | Field Work Started | Planned | Terms of Reference agreed by management December 2023. Field work commenced March 2024, as agreed with management. |
| 8 | 2 | 2 | Communities | Damp and Mould - Housing Stock | Assurance | High | Final Report | Final Report Issued | Reported to September 2023 Committee. |
| 9 | 2 | N/A | Communities | Housing Management System-Project Management | Assurance | High | Deferred | Deferred | Management request for activity deferral due to service review within 2023-24. |
| 10 | 2 | N/A | Resources | Phase 3b Decarbonisation Scheme | Assurance | High | Cancelled | Planned | Audit cancelled as funding body have confirmed that audit certification is not required. |
| 11 | 2 | N/A | Communities | Homelessness Prevention | Assurance | High | Deferred | Deferred | Management request for activity deferral due to service review within 2023-24. |
| 12 | 2 | N/A | Place | Developer Contributions | Assurance | High | Deferred | Planned | Management request for activity deferral due to lead officer turnover. |
| 13 | 2 | 2 to 3 | Communities | Changing Places Fund Grant Determination | Assurance | Medium | Final Report Issued | Final Report Issued | Reported to January 2024 Committee. |
| 14 | **NEW** | 2 | Resources | Council Tax Energy Support Grant | Assurance | High | Final Report Issued | Final Report Issued | This audit was requested by Strategic Director of Resources, due to the Department for Levelling Up, Housing and Communities requesting sight of an Internal Audit report. Reported to September 2023 Committee. |
| 15 | **NEW** | 3 | Resources & Place | Contain Outbreak Management Fund (COMF) | Assurance | High | Final Report Issued | Final Report Issued | Reported to January 2024 Committee. |
| 16 | **NEW** | 3 to 4 | Place | Disabled Facilities Grant (DFG) | Assurance | High | Field Work Started | Field Work Started | Draft report to be issued by March 2024 month end. |
| 17 | 3 | 3 to 4 | Resources | Risk Management Follow-Up | Assurance | High | Final Report Issued | Field Work Started | Final report issued to management in February 2024. |
| 18 | 3 | N/A | Place | Damp and Mould Private Sector | Assurance | High | Deferred | Deferred | Head of Environmental Health and Housing Renewal Manager request for Disabled Facilities Grant audit to be prioritised and Damp and Mould Private Sector to be deferred based on in year risk assessment. Agreement obtained from the Strategic Director of Place. |
| 19 | 3 | N/A | Resources | ICT Asset Management | Assurance | High | Deferred | Deferred | Following discussions with ICT Management it has been requested that this audit is deferred to 2024-25 to feed into the audit planning risk assessment. |
| 20 | 3 | N/A | Resources | Cash and Bank | Assurance | High | Deferred | Planned | Following discussions with management it has been requested that this audit is deferred to 2024-25 to feed into audit planning risk assessment. |
| 21 | 3 | 3 | Resources | Brimscombe Port Management Accounts | Assurance | Medium | Final Report Issued | Final Report Issued | Reported to January 2024 Committee. |

**Stroud District Council 2023-24 Internal Audit Progress Report - April 2024**

| Ref | Plan Quarter | Actual Quarter | Dept. | Audit | Comment | Risk | Status Now | Status Last Report | Comments |
|---|---|---|---|---|---|---|---|---|---|
| 22 | 4 | N/A | Communities | Housing Revenue Account Delivery Plan | Assurance | High | Deferred | Planned | Following discussions with management it has been requested that this audit is deferred to 2024-25 to feed into audit planning risk assessment. |
| 23 | 4 | 4 | Communities | Business Continuity | Assurance | High | Field Work Started | Planned | Terms of Reference issued and field work commenced in February 2024. |
| 24 | 4 | 4 | Resources | ICT Disaster Recovery and Cyber Incident Response Arrangements Follow-Up | Assurance | High | Field Work Started | Planned | Field work commenced in March 2024. |
| 25 | 4 | 4 | Resources | ICT Security Information and Event Management Process | Assurance | High | Field Work Started | Planned | Terms of Reference issued in January 2024 and field work commenced in February 2024. |
| 26 | 4 | N/A | Resources | People Strategy | Assurance | High | Deferred | Planned | Following discussions with management it has been requested that this audit is deferred to 2024-25 to feed into audit planning risk assessment. |
| 27 | 4 | N/A | Communities | Emergency Planning | Assurance | High | Deferred | Planned | Following discussions with management it has been requested that this audit is deferred to 2024-25 to feed into audit planning risk assessment. |
| 28 | 4 | 4 | Resources | National Non-Domestic Rates - Opening Debits | Assurance | High | Field Work Started | Planned | Terms of Reference issued in January 2024 and field work commenced in March 2024. |
| 29 | 4 | 4 | Resources | Council Tax - Opening Debits | Assurance | High | Field Work Started | Planned | Terms of Reference issued in January 2024 and field work commenced in February 2024. |
| **Work Planned for Throughout 2023-24** | | | | | | | | | |
| 30 | Throughout | Throughout | Resources | Grants - Contingency | Grants | High | Ongoing | Ongoing | Provision for reviews to assess the effectiveness of the governance arrangements to ensure compliance with the terms and conditions of the grant. |
| 31 | Throughout | Throughout | Communities | Leisure Facilities - Local Authority Trading Company | Consultancy | High | Ongoing | Ongoing | Provision of risk and control advice as part of the future program for introducing the Local Authority Trading Company. |
| 32 | Throughout | 2 | Resources | Post Payment Assurance | Assurance | High | Final Report Issued | Final Report Issued | Delivered through the Council Tax Energy Scheme activity - row ref 14. Council Tax Support Scheme review to be included in the 2024-25 audit planning risk assessment. |
| 33 | Throughout | Throughout | Counter Fraud | Counter Fraud | Assurance | High | Ongoing | Ongoing | Counter Fraud activity progresses throughout the year and is reported at each Committee. |

| Key: | | | | |
|---|---|---|---|---|
| | 🟩 | The audit has started or will start on time. | TBC: | To be confirmed. |
| | 🟧 | The audit commencement has been or is likely to be delayed. | N/A: | Not applicable. |
| | 🟥 | The audit is not likely to be undertaken in this financial year. | C/fwd: | Carried forward from 2022-23 |

Agenda Item 16
Appendix C