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

Monday, 19 April 2021

AUDIT AND STANDARDS COMMITTEE

A remote meeting of the Audit and Standards Committee will be held on **TUESDAY, 27 APRIL 2021** at **7.00 pm**

Kathy O'Leary
Chief Executive

This is a remote meeting in accordance with the Local Authorities and Police and Crime Panels (Coronavirus) (Flexibility of Local Authority and Police and Crime Panel Meetings) (England and Wales) Regulations 2020.

Venue
This meeting will be conducted using Zoom and a separate invitation with the link to access the meeting will be sent to Members, relevant officers and members of the public who have submitted a question.

Public Access
Members of the public, who have not submitted a question, are invited to access the meeting streamed live via Stroud District Council's YouTube channel.

Recording of Proceedings
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.

A G E N D A

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

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

3. **MINUTES (Pages 5 - 8)**
   To approve the minutes of the meeting held on 26 January 2021.

4. PUBLIC QUESTION TIME

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 Thursday, 22 April 2021

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. AUDIT AND STANDARDS COMMITTEE ANNUAL REPORT 2020/21 (Pages 9 - 24)

The Annual Report summarises the activities of the Audit and Standards Committee during 2020/21 and sets out its plans for the next twelve months. This report provides an independent assurance that the Council has in place adequate and effective governance, risk management and internal control frameworks; Internal and External Audit functions; and financial reporting arrangements that can be relied upon and which contribute to the high corporate governance standards that this Council expects and maintains.

6. INTERNAL AUDIT ACTIVITY PROGRESS REPORT 2020/21 (Pages 25 - 50)

To inform Members of the Internal Audit activity progress in relation to the approved Revised Internal Audit Plan 2020/21.

7. DRAFT INTERNAL AUDIT PLAN 2021/22 (Pages 51 - 80)

To provide the Committee with a summary of the draft Risk Based Internal Audit Plan 2021/22 as required by the Accounts and Audit Regulations 2015 and the Public Sector Internal Audit Standards (PSIAS) 2017.

8. CREDITORS LIMITED ASSURANCE UPDATE (Pages 81 - 96)

To receive updates from Senior Officers on the above.

9. 3RD QUARTER TREASURY MANAGEMENT ACTIVITY REPORT 2020/21 (Pages 97 - 106)

To provide an update on Treasury Management activity as at 31 December 2020.

10. COUNTER FRAUD UNIT REPORT AND REGULATION OF INVESTIGATORY POWERS ACT (RIPA) 2000 / INVESTIGATORY POWERS ACT (IPA) 2016 REPORT (Pages 107 - 160)

To provide the Audit and Standards Committee with assurance over the counter fraud activities of the Council in relation to the work undertaken by the Counter Fraud Unit (CFU).

11. Standing Items

(a) To consider any Risk Management issues

12. MEMBER QUESTIONS

See Agenda Item 4 for deadlines for submission.

Members of Audit and Standards Committee

Councillor Nigel Studdert-Kennedy (Chair)
Councillor Dorcas Binns
Councillor Miranda Clifton
Councillor Stephen Davies
Councillor Colin Fryer

Councillor Tom Williams (Vice-Chair)
Councillor Karen McKeown
Councillor Keith Pearson
Councillor Mark Reeves

This page is intentionally left blank

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

3

AUDIT AND STANDARDS COMMITTEE

26 January 2021

7.00 pm – 7.57 pm

Remote Meeting

Minutes

Membership

Councillor Nigel Studdert-Kennedy (Chair)	P	Councillor Colin Fryer	P
Councillor Tom Williams (Vice-Chair)	P	Councillor Karen McKeown	A
Councillor Dorcas Binns	P	Councillor Keith Pearson	P
Councillor Miranda Clifton	P	Councillor Mark Reeves	P
Councillor Stephen Davies	P		

A = Absent P = Present

Officers in Attendance

Strategic Director of Resources
Principal Accountant
Monitoring Officer
Housing Strategy and Community Infrastructure Manager
Head of Audit Risk Assurance (ARA)
Group Manager, ARA
Senior Democratic Services and Elections Officer
Democratic Services and Elections Officer

AC.045 APOLOGIES

An apology for absence was received from Councillor McKeown.

AC.046 DECLARATIONS OF INTEREST

There were none.

AC.047 MINUTES

RESOLVED That the Minutes of the meetings held on 17 November 2020 are approved as a correct record.

AC.048 PUBLIC QUESTION TIME

There were none.

AC.049 INTERNAL AUDIT ACTIVITY PROGRESS REPORT 2020/21

The Group Manager, ARA presented the report and highlighted its reference to:

- Concluded Internal Audit activities from November and December 2020
- Special investigations/counter fraud activity update for the respective period
- Additional/new activities progressed by ARA due to the risks and impact of Covid-19

There were two main assurance outcomes within the report; the independent assurance provision required on specific data for the Ofgem application, and the split assurance opinion on risk regards tenancy lettings (split due to limited assurance being applied in relation to a specific area of risk). Members were informed that wider Plan activity was progressing well. Based on the level of new assurance activities coming through in-year due to Covid-19 risk areas/themes (e.g. the work associated with Covid-19 business grants which had input from both the Internal Audit and Counter Fraud teams), the Group Manager, ARA confirmed that request for audit/activity deferral was likely to be seen in the April 2021 report to Committee, based on risk and to ensure provision of the approved Plan days.

Councillor Binns enquired were the issues highlighted by the limited assurance to do with Covid-19. The Group Manager, ARA confirmed that the audit had resulted in five recommendations. Two recommendations were high-priority and both related to risk management themes within risk identification and management arrangements for tenancy lettings, regards the Locator system and a business continuity plan for the Homeseekerplus policy. These were the main reasons for the limited assurance being applied to that ring fenced area within tenancy lettings. Councillor Binns further examined whether this would get worse further into 2021 due to the pandemic. The Housing Strategy and Community Infrastructure Manager affirmed that in terms of the operational position, the greatest fear was losing capacity through staff. The limited assurance therefore needed to be addressed particularly keenly in the current time. The Locator system and Homeseekerplus were county-wide provisions so this would be a good opportunity to work with county council on investigation. The computer system was designed to be very robust; it was a cloud-based system held on duplicate servers in different locations. Work was planned to ensure all the contingency plans necessary would be put in place for this service area. The Group Manager, ARA added that a follow up audit for review of the recommendations would be included in the proposed 2021/22 audit plan.

Following a show of hands, the Chair confirmed that the Motion was carried.

RESOLVED **To note:**

a) The progress against the Revised Internal Audit Plan 2020/21; and

b) The assurance opinions provided in relation to the effectiveness of the Council's control environment.

AC.050 **ANNUAL GOVERNANCE STATEMENT 2019/20 IMPROVEMENT PLAN – PROGRESS REPORT**

The Group Manager, ARA explained that the 2019/20 Annual Governance Statement included three governance actions. The Progress Report being considered at this Committee was an update to confirm the progression made to date against the actions identified in the 2019/20 Statement. The Progress Report had been facilitated by ARA and included update per action as provided by the specific lead Officers, or their nominated deputies. A final update against the actions was due to be confirmed by the 2020/21 Annual Governance Statement, which would come through to Committee in June-July 2021.

Councillor Davies asked how Covid-19 had impacted on this; had it been possible to continue with the strategy or had it been badly affected by the pandemic. The Strategic Director of Resources informed Members that the peer challenge report was split into two parts. A lot of short-term actions were included, including the formation of a new leadership team, and these

were largely all completed by March 2020. For a lot of the longer-term actions involved, such as forming a new Corporate Delivery Plan, progress had happened in a slightly different way to that anticipated, partly as a result of the cancellation of the 2020 Elections. The Council did not yet have a new Corporate Delivery Plan but there was a Council Recovery Strategy which did set out many current objectives. Changes and delays that had occurred with long-term actions from the report would be looked at over the coming year.

Following a show of hands, the Chair confirmed that the Motion was carried.

RESOLVED **To note the progress made against the identified improvement areas.**

AC.051 **TREASURY MANAGEMENT STRATEGY, ANNUAL INVESTMENT STRATEGY AND MINIMUM REVENUE PROVISION POLICY STATEMENT 2021/22**

The Principal Accountant outlined the report, which accompanied the recently formulated capital and revenue budgets, and highlighted features including:

- A focus on the capital programme, the financing thereof, and the levels of planned borrowing that arose from the estimates going through the budgeting process, which was in the region of £30 million;
- The concurrent debt repayment element regards previous borrowing, which was the result of the Minimum Revenue Provision payments and in the region of £10 million;
- The strategy to increase internal borrowing to obtain an interest rate benefit, since interest rates were low, with the base rate at 0.1%, meaning Council investments were achieving low interest returns in the present environment. Advice sought with Link had suggested this was likely to prevail until March 2024 at the earliest.

There were two proposed changes to the investments that the Council allowed itself to utilise:

- To increase the limit to specified investments with local authorities from £8 million to £12 million, since rates in this active market were higher than for traditional investments, and
- A total of £8 million on unrated building societies within non-specified investments, subject to a maximum of £2 million for up to 6 months for an unrated building society with assets of greater than £1 billion, and a maximum of £1 million for up to 3 months for an unrated building society with assets under £1 billion.

All else in the investment categories remained unchanged. Paragraph 5.1 reported on the new contract with Link which had commenced on 1 October 2020. This would run to 30 September 2023, with the option to extend, on mutually-agreed terms, to 30 September 2025 if required.

Councillor Davies asked for further detail regards the wide variances year-on-year within capital expenditure. Members were informed that this would be addressed at the next Strategy and Resources Committee. Councillor Davies requested further explanation for Table 5. The Principal Accountant explained that the borrowing costs in 2019/20 were 15% and had been reducing since. The indicator also included investment income. The General Fund had much lower borrowing so the income from investments exceeded the interest on borrowing. This resulted in an effective net income to the General Fund. Councillor Binns asked for an explanation of the fluctuations in Table 3a. The Principal Accountant confirmed that details would be circulated to Members following the meeting.

Councillor Bins enquired, if interest rates were to stay at a low level, whether the Council could take a risk and invest somewhere else in order to get a better return. The Principal Accountant explained that the strategy was being set here and that would be the approach the Treasury team would take. The Strategic Director of Resources informed Members of a change introduced in recent years of setting up to £15 million, previously £10 million, for a wider range of risks and

pooled funds. There was always a balance to be struck and the finance team were working hard to offset the impact of the fall in interest rates. To a further query about whether the Council could make more innovative investments such as through private means, the Strategic Director of Resources confirmed that this would be possible but there would be many legal caveats and restrictions; it did not currently feature in the Council's capital programme.

The Chair asked for the approximate average returns for the last 12 months on the Lothbury, Hermes and multi-asset Royal London and CLA funds. The Principal Accountant informed Members that these were 2.3% to 2.5% on £10 million, much better compared to the bank rate of 0.1%. The Chair further enquired, given Covid-19, whether it was expected that the capital programme would be spent. The Strategic Director of Resources answered that the capital programme was realistic and what was considered reasonable and achievable had been set out. There was currently a greater risk exposure due to Covid-19; it was important to be aware of the potentially increased risks associated with the canals project, new homes strategy and Brimscombe Port development particularly, which could be complicated by the pandemic. Changes may occur and in-year monitoring and reporting on progress would be carried out.

On being put to the vote, the motion was carried unanimously.

RECOMMENDED TO COUNCIL

a) To adopt the prudential indicators and limits for 2021/22 to 2023/24
b) To approve the Treasury Management Strategy 2021/22, and the treasury prudential indicators;
c) To approve the Investment Strategy 2021/22, and the detailed criteria for specified and non-specified investments, and
d) To approve the MRP Statement 2021/22

AC.052 STANDING ITEMS

(a) Work Programme: The Group Manager, ARA made a request to Committee for consideration, due to the pandemic, for the Review of the Effectiveness of the Audit and Standards Committee report to be deferred, removed from the 27 April 2021 agenda, and included instead in the 2021/22 Work Programme. This would be to enable an appropriate position to be reported on to Committee at that time, once the definitive actions occurring on Elections and wider matters were known. No comments against this were raised and the Chair confirmed that the Committee accepted this suggestion. The Strategic Director of Resources also reported that Emma Cathcart of the Counter Fraud Unit had an update report on Counter Fraud Activity for Members' consideration at Committee on 27 April 2021. It was agreed that this report should be included in the agenda in replacement of the deferred report.

(b) Risk Management: The Chair pointed out the highlighted risks on Excelsis, which were familiar and previously seen. No immediate adjustment was required. The Strategic Director of Resources confirmed that work was planned to update the strategic risks. The Strategic Leadership Team would be receiving updates and these would be reported on to Members.

AC.053 MEMBERS' QUESTIONS

There were none.

The meeting closed at 7:57 pm.

Chair

STROUD DISTRICT COUNCIL **AGENDA ITEM NO**

AUDIT AND STANDARDS COMMITTEE

27 APRIL 2021 **5**

Report Title	**AUDIT AND STANDARDS COMMITTEE ANNUAL REPORT 2020/21**
Purpose of Report	The Chartered Institute of Public Finance Accountants (CIPFA) 'Practical Guidance for Local Authorities and Police – 2018 Edition' includes a position statement which states that audit committees should: 'report regularly on its work to those charged with governance [Full Council], and at least annually report an assessment of their performance. An annual public report should demonstrate how the committee has discharged its responsibilities'. This Annual Report fulfils the above requirement. The Annual Report summarises the activities of the Audit and Standards Committee during 2020/21 and sets out its plans for the next twelve months. This report provides Council with an independent assurance that the Council has in place adequate and effective governance, risk management and internal control frameworks; Internal and External Audit functions; and financial reporting arrangements that can be relied upon and which contribute to the high corporate governance standards that this Council expects and maintains.
Decision(s)	**That the Committee:** **a) RESOLVES to agree the Audit and Standards Committee Annual Report 2020/21; and** **b) RECOMMENDS to Council that the Annual Report 2020/21 be approved.**
Consultation and Feedback	All Members of the Audit and Standards Committee have been consulted on the report content.
Report Author	Piyush Fatania Head of Audit Risk Assurance Tel: 01452 328883 Email: piyush.fatania@gloucestershire.gov.uk

Options	Consideration has been given to not producing an Annual Report however this has been discounted due to the requirement stated above.			
Background Papers	Relevant public reports presented to the Audit and Standards Committee during 2020/21 and minutes of those meetings can be found via the following link: https://www.stroud.gov.uk/council/meetings/audit-standards-committee			
Appendices	Appendix A – Audit and Standards Committee Annual Report 2020/21			
Implications (details at the end of the report)	Financial	Legal	Equality	Environmental
	No	No	No	No

1.0 INTRODUCTION/BACKGROUND

1.1 Stroud District Council is responsible for ensuring that its business is conducted in accordance with the law and proper standards and that public money is safeguarded, properly accounted for and used economically, efficiently and effectively. In discharging this overall responsibility, the Council is responsible for putting in place the proper arrangements for the governance of its affairs.

1.2 A sound corporate governance framework involves accountability to service users, stakeholders and the wider community, within which the Council takes decisions and leads and controls its functions to achieve stated objectives and priorities. It thereby provides an opportunity to demonstrate the positive elements of the Council's business and to promote public confidence.

1.3 Audit Committees are widely recognised as a core component of effective governance. Their key role is independently overseeing and assessing the internal control environment, comprising governance, risk management and control and advising the Council on the adequacy and effectiveness of these arrangements.

1.4 In response to the above, the Audit and Standards Committee was established in September 2009 in line with guidance issued by the Chartered Institute of Public Finance and Accountancy (CIPFA). This guidance recommends that audit committees should prepare an annual report to the full Council, which sets out the Committee's work on how they have discharged their responsibilities.

2.0 MAIN POINTS

2.1 The Committee undertakes a substantial range of activities and works closely with the Chief Financial Officer (Section 151 Officer) and both Internal and External Auditors, in achieving the Council's aims and objectives. The Committee has developed and implemented a work plan for the year to enable key tasks to be considered, undertaken and delivered. To summarise, through the work plan the Committee has:

- Provided independent assurance on the adequacy of the governance, risk management framework and associated control environment;

- Provided independent scrutiny of the Council's financial and non financial performance to the extent that it affects the Council's exposure to risk and weakens the control environment; and
- Overseen the statutory financial reporting process.

3.0 CONCLUSION

3.1 The Audit and Standards Committee has had a successful year in providing the Council with assurances on the strength of its governance and stewardship arrangements and in challenging those arrangements.

3.2 The Committee's work programme is a dynamic programme and will continue to be reviewed to ensure the Committee maximises its contribution to the governance and control framework at the same time managing agendas to ensure that all meetings are focused on the key issues.

4.0 IMPLICATIONS

4.1 Financial Implications

There are no financial implications arising directly from this report.

Andrew Cummings, Strategic Director of Resources
Tel: 01453 754115
Email: andrew.cummings@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 arising from this report.

Contact detail: Patrick Arran, Monitoring Officer
One Legal
Email: patrick.arran@stroud.gov.uk

4.3 Equality Implications

There are no equality implications as a result of the recommendations made within this report.

4.4 Environmental Implications

There are no environmental implications as a result of the recommendations made within this report.

This page is intentionally left blank

Audit and Standards Committee Annual Report 2020/21

Contents

Statement from the Chairman of the Audit and Standards Committee

The committee has met formally six times via the Zoom link. Despite the restrictions placed on it by the pandemic considerable progress was made. Meeting on 26th May 2020 approved the Internal Audit Plan subject to caveats regarding redeployment of officers to Pandemic duties and changing requirements. At the meeting in July 2020 it was confirmed by the Monitoring Officer that the Code of Conduct was in the remit of the Audit and Standards Committee. It was also confirmed that it had been agreed at Council that the draft Code of Conduct and the arrangements under which allegations under the Code of Conduct were investigated was to be reviewed by the Audit and Standards Committee. An extraordinary meeting took place on Tuesday 25th August 2020 to review and make recommendations in this regard. The Interim Head of Legal Services and Monitoring Officer confirmed that the Committee were being asked to consider the draft amended Code of Conduct and Arrangements for Investigating Complaints appended to the report and, subject to any changes it wished to make:

a) Recommend them to the next meeting of Council for adoption; and

b) Authorise the Monitoring Officer to provide town and parish councils with the proposed process for investigating complaints for information and comment prior to consideration by Council at its next meeting.

At the next meeting of Council, held on 22nd October 2020, the Proposed Amendments to the Code of Conduct for Members and the Arrangements under which Allegations Can Be Investigated were proposed. Upon being put to the vote the Motion was unanimously carried: *'RESOLVED To adopt the amended Code of Conduct and Arrangement for investigation alleged breaches of the Code with immediate effect.'*

The Committee has also considered regular reports on Treasury Management and Risk Management, Procurement, Fraud and Internal Audit Progress Reports and the Annual Statement of Accounts and Annual Governance Report.

During the year we said goodbye to Cllrs Rachel Curley and Trevor Hall who moved to different duties and welcomed Cllr. Miranda Clifton and the return of Cllr. Colin Fryer. We thank all of them and wish them well.

We also said goodbye to Theresa Mortimer, Head of A.R.A., the author of many Internal Audit Reports and procedures, who retired in December 2020.

We also welcomed Theresa Mortimer's successor in post, Piyush Fatania who joined us in January 2021.

Finally, I would like to convey my thanks to all the members of the Committee, both current and recent, and to the officers for all the work done during the past year. While the work was performed under somewhat challenging circumstances the results have justified the effort.

I would also like to thank Democratic Services without whom neither visual nor written communication would have been so smooth, if possible at all.

Cllr. Nigel Studdert-Kennedy,

Audit and Standards Committee

09/03/2021

Background

The Council entered the 2020/21 financial year in the midst of the Covid-19 pandemic. In its response to this, the Council has followed guidance from the government. This has included:

(i) Asking the majority of staff to work from home;

(ii) Redeploying a number of staff from their normal roles to assist in the Council's response; and

(iii) Paying emergency and discretionary grants to local businesses on behalf of the government.

Internal Audit provided assistance in the work for (iii) above with pre and post payment checks.

The Committee has continued throughout the pandemic to oversee the Council's work on risk management, capital projects, treasury management and anti-fraud. The Committee delivered this through holding virtual meetings within the year, in line with the dates confirmed in the 'Membership and Meetings' report section.

The pandemic has necessitated the amendment of the Annual Internal Audit Plan and this has been overseen and agreed by the Committee.

Stroud District Council is responsible for ensuring that its business is conducted in accordance with the law and proper standards and that public money is safeguarded, properly accounted for and used economically, efficiently and effectively. In discharging this overall responsibility, the Council is responsible for putting in place the proper arrangements for the governance of its affairs.

A sound corporate governance framework involves accountability to service users, stakeholders and the wider community, within which the Council takes decisions and leads and controls its functions to achieve stated objectives and priorities. It thereby provides an opportunity to demonstrate the positive elements of the Council's business and to promote public confidence. Audit Committees are widely recognised as a core component of effective governance.

The Audit and Standards Committee is responsible for overseeing the Council's corporate governance, audit and risk management arrangements. The Committee is also responsible for approving the Statement of Accounts and the Annual Governance Statement. The Committee's specific powers and duties are set out in Council's Constitution.

The Chartered Institute of Public Finance and Accountancy (CIPFA) issued guidance to local authorities to help ensure that Audit Committees are operating effectively[1]. The guidance recommends that audit committees should report annually on how they have discharged their responsibilities. The key benefits to the Council of operating an effective Audit and Standards Committee are:

[1] CIPFA – Practical Guidance for Local Authorities and Police, 2018

- Maintaining public confidence in the objectivity and fairness of financial and other reporting;
- Reinforcing the importance and independence of Internal and External Audit and any other similar review process;
- Providing a focus on financial reporting both during the year and at year end, leading to increased confidence in the objectivity and fairness of the financial governance arrangements operating within the Council;
- Assisting the co-ordination of sources of assurance and, in so doing, making management more accountable;
- Providing additional assurance through a process of independent and objective review, via the Internal Audit function;
- Raising awareness within the Council of the need for governance, including ethical governance, internal control and the implementation of audit recommendations; and
- Providing assurance on the adequacy of the Council's risk management arrangements, including the risk of fraud and irregularity.

Membership and Meetings

The Committee has enjoyed the benefit of a relatively settled membership over the last three years. This has helped to build and retain the expertise within the Committee, which has led to the Committee being able to demonstrate that they are operating within a best practice framework.

There are nine Members of the Audit and Standards Committee namely:

- Councillor Nigel Studdert-Kennedy (Chair)
- Councillor Tom Williams (Vice Chair)
- Councillor Dorcas Binns
- Councillor Colin Fryer
- Councillor Stephen Davies
- Councillor Keith Pearson
- Councillor Miranda Clifton
- Councillor Mark Reeves
- Councillor Karen McKeown

During the 2020/21 financial year, the Audit and Standards Committee has met on six occasions, in accordance with its Programme of Work:

- 26th May 2020
- 29th July 2020
- 25th August 2020
- 6th October 2020
- 17th November 2020
- 26th January 2021

In addition, the Annual Report is being presented to the 27th April 2021 Audit and Standards Committee meeting.

The Committee is also supported by Council officers, principally the Chief Financial Officer (S151 Officer), Monitoring Officer, Head of Audit Risk Assurance (Chief Internal Auditor) and the Council's External Auditors (Deloitte).

Work Programme

During this period, the Committee has assessed the adequacy and effectiveness of the Council's risk management arrangements, control environment and associated counter fraud arrangements through regular reports from officers, the Internal Auditors (Audit Risk Assurance) and the External Auditors (Deloitte).

The Committee has sought assurance that action has been taken, or is otherwise planned by management to address any risk related issues that have been identified by the auditors during this period.

The Committee has also sought to ensure that effective relationships continue to be maintained between the Internal and External Auditors and between the auditors and management. The specific work undertaken by the Committee during 2020/21 is set out below.

Internal Audit Activity

With effect from May 2016, the Internal Audit service is provided by Audit Risk Assurance under a shared service agreement. The Committee has continued to monitor the work of Internal Audit and has:

- Considered the effectiveness of the Audit Risk Assurance Shared Service;
- Contributed towards, received and approved the Internal Audit Plan for 2020/21. The same actions have been completed by Committee for the Revised Internal Audit Plan 2020/21. Covid-19 has placed significant pressures on Council services and has impacted (and continues to impact) the Council's priorities, objectives and risk environment. Due to the changing position and to ensure that the Risk Based Internal Audit Plan met the assurance needs of the Council, the Revised Risk Based Internal Audit Plan 2020/21 was approved by Audit and Standards Committee on 6th October 2020. The plan ensures that Internal Audit resources are prioritised towards those systems, processes and areas which are considered to be deemed high risk, or which contribute most to the achievement of the Council's corporate objectives;
- Participated in the 2021/22 Internal Audit Risk Based Planning workshop to contribute towards the Internal Audit plan and audit resource allocation to support assurance needs;
- Monitored the delivery of the annual Internal Audit Plan through regular update reports presented by the Head of Audit Risk Assurance;

- Received, considered and monitored the results of internal audits performed and high risk activity identified, in respect of specific areas where a limited opinion on the control environment has been provided, e.g. the Electrical Works Contract activity and monitored the progress made by management, during the period, to address identified control weaknesses;
- Approved the Council's overall counter fraud arrangements and response in the light of national guidance Fighting Fraud and Corruption Locally – The Local Government Counter Fraud and Corruption Strategy which is supported by CIPFA Counter Fraud Centre, with the principles reflected in the Council's updated Anti Fraud and Corruption Strategy 2020 - 2023;
- Received updates on the outcomes of special investigations undertaken by Internal Audit, along with progress made in the investigation of queries arising as a result of the National Fraud Initiative (NFI) data matching exercise;
- Furthered discussion on relevant key themes, following consideration and approval of the report of the Head of ARA on the service's purpose, authority, role and function in January 2020.; and
- Considered the Internal Audit Annual Report 2019/20 of the Head of Audit Risk Assurance, which provided a satisfactory opinion on the effectiveness of the Council's internal control environment and summarised the Internal Audit activity upon which that opinion was based. The Committee can therefore take reasonable assurance that there is a generally sound system of internal control in place at the Council.

In addition, the Committee received the outcomes from the External Quality Assessment of the Effectiveness of Internal Audit within year.

There is a requirement under the Public Sector Internal Audit Standards (PSIAS) i.e. Standard Ref '1312 External Assessments' for Internal Audit to have an external quality assessment which must be conducted at least once every five years by a qualified, independent assessor or assessment team from outside the organisation. The Standards require the Head of Audit Risk Assurance (the Chief Internal Auditor) to discuss the following with the relevant Audit Committee:

- The form of external assessment; and
- The qualifications and independence of the external assessor or assessment team, including any potential conflict of interest.

The latest review was undertaken during May 2020 by the Chartered Institute of Internal Auditors (CIIA) and reported to Audit and Standards Committee within 2020/21. The relevant 29th July 2020 Audit and Standards Committee minutes document the following:

'AC.013: INTERNAL AUDIT EXTERNAL QUALITY ASSESSMENT (EQA) - OUTCOME

The Approved Reviewer for the Chartered Institute of Internal Auditors (CIIA) informed Members of the outcome of the independent assessment of the Internal Audit function. The output report provided an opinion on how well the audit service worked in line with these standards. The review was undertaken in May by a survey of and interviews with key stakeholders that was a very detailed and diligent exercise.

The end result was that the Council have an excellent Internal Audit service providing them with a good range of consultation as the team undertake their work. The results of the quality assessment showed that this was one of the best Internal Audit services he had had the privilege of reviewing. This was a good news story that the service were operating fully within the international standards. Congratulations were conveyed by the Approved Reviewer, the Chair and Committee to the Head of Audit Risk Assurance (ARA) and her team.'

Activity relating to Treasury Management

During the year, the Audit and Standards Committee have:

- Received and approved the quarterly and half yearly Treasury Management activity reports which monitor treasury activity against the 2020/21 strategy.
- Also considered and recommended to full council the annual report setting out the Treasury Management Strategy, the Annual Investment Strategy and Minimum Revenue Provision Policy Statement 2021/22. This report also set the Council's prudential indicators for 2021/22.
- Treasury Management is a key area for the Committee to monitor and they continue to consider and recommend to full Council for approval amendments to the investment strategy in response to constantly changing market conditions. The 2019/20 Investment Strategy recommended by Committee included a number of new investment options as the Council increased its risk appetite, and the Committee is monitoring the £10m of longer term investments in property funds and multi-asset funds arising from that change.

External Audit Activity

Deloitte was appointed as the Council's External Auditors for the financial years 2018/19, 2019/20 and 2020/21. The Committee (either via full Committee and/or delegated responsibility of the Chair) has monitored the work of the Council's External Auditors and has:

- Considered and accepted the Annual Audit Letter 2019/20 (through the November 2020 Committee meeting). This letter summarises the outcome from audit work at the Council during this period;
- Considered the Internal Audit / External Audit joint working arrangements;
- Received and considered regular External Audit progress reports; and
- Considered the draft Statement of Accounts for 2019/20 of the Council (through the November 2020 Committee meeting) and have received verbal updates on the position of External Audit.

It is noted that at the point of drafting the Audit and Standard Committee Annual Report 2020/21, the 2019/20 Statement of Accounts and relevant External Audit opinions and External Audit Report 2019/20 (the 'Report to those charged with Governance' in accordance with the requirements of International Standard on Auditing 260) are due to be concluded.

Risk Management Activity

During the year the Committee has:

- Received regular risk management relevant update reports; and
- Included risk management as a standing agenda item for all Audit and Standards Committee meetings.

Corporate Governance

In relation to corporate governance the Committee:

- Has continued to lead the review of the effectiveness of the Audit and Standards Committee and progression of the identified improvement actions i.e. the key proposed actions relating to the appointment of an independent member to the Committee and refresh of the Committee's terms of reference to reflect the revised CIPFA guidance (with further update to Committee expected in July 2021); and
- Considered and approved the Council's 2019/20 Annual Governance Statement and Local Code of Corporate Governance. The Committee also reviewed the progress made by management to address the required actions identified in the 2019/20 Annual Governance Statement Improvement Plan.

Training

The following training was made available to Members of the Audit and Standards Committee in 2020/21 to support the Committee in discharging its responsibilities:

- Equality and Diversity Training - Online training provided by LGA
  Mandatory for all Members
  17th June 2020

- GDPR - Online GDPR course provided by MY Learning via SDC
  Mandatory for all Members who hadn't completed it in the last 12 months
  30th June 2020

- Race Relations and Inclusive Leadership – Zoom training session delivered by ENEI (Employer
  Mandatory for all Members
  21st, 27th and 28th July 2020

- Lothbury Property Trust Fund Briefing
  Open to all Members
  6th October 2020

- Planning White Paper and Local Plan Briefing
  Open to all Members
  7th October 2020

- CIL Strategic Infrastructure Funding – Members Information Session
  Open to all Members
  25th November 2020

- Fusion Briefing
  Open to all Members
  15th December 2020

- Risk Based Internal Audit Planning Workshop
  Open to Audit and Standards Committee
  26th January 2021

- Strategy for Leisure, Health and Wellbeing Consultation Briefing
  Open to all Members
  28th January 2021

- Ascend Organisational Development Programme – Fit for the Future
  Open to all Members
  February-March 2021

- Census 2021: All-Member Briefing
  Open to all Members
  2nd March 2021

- UBICO Seminar
  Open to all Members
  4th February 2021

- Brimscombe Port Redevelopment Update
  Open to all Members
  17th February 2021

- Beyond Covid: Race, Health and Inequality in Gloucestershire - All-Member Briefing with Director of Public Health, Gloucestershire
  Open to all Members
  9th March 2021

- Fusion Briefing - Fusion Power Plant and opportunities at Berkeley and Oldbury
  Open to all Members
  16th March 2021

- Informal briefing on the Youth Service being led by Youth Representatives and Youth Officers of Stroud District Council
  Open to all Members
  15th April 2021

Future Work

During 2021/22, the Audit and Standards Committee will continue with the existing aim of being an important source of assurance about the organisation's arrangements for managing risk, maintaining an effective control environment, and reporting on financial and other performance.

In particular, they will continue to support the work of Internal and External Audit and ensure appropriate responses are given to their recommendations and continue to monitor any actions arising from the Annual Governance Statement action plan 2020/21, to ensure the Council's governance arrangements are effective.

In addition, with risk management being a key contributor to good governance the Committee will be seeking independent assurance from Internal Audit that risk management continues to be embedded within the Council's key business processes.

Conclusion

The Audit and Standards Committee has had a successful year in providing the Council with assurances on the strength of its governance and stewardship arrangements and in challenging those arrangements.

The Committee's work programme is a dynamic programme and will continue to be reviewed to ensure the Committee maximises its contribution to the governance and control framework, at the same time managing agendas to ensure that all meetings are focused on the key issues.

Details of all reports as noted within the Audit and Standards Committee Annual Report 2020/21 can be found at: https://www.stroud.gov.uk/council-and-democracy/meetings/audit-standards-committee

This page is intentionally left blank

STROUD DISTRICT COUNCIL

AGENDA ITEM NO

AUDIT AND STANDARDS COMMITTEE

27 APRIL 2021

6

Report Title	**INTERNAL AUDIT ACTIVITY PROGRESS REPORT 2020/21**			
Purpose of Report	To inform Members of the Internal Audit activity progress in relation to the approved Revised Internal Audit Plan 2020/21.			
Decision(s)	**The Committee RESOLVES to note:** **a) The progress against the Revised Internal Audit Plan 2020/21; and** **b) The assurance opinions provided in relation to the effectiveness of the Council's control environment.**			
Consultation and Feedback	Internal Audit findings are discussed with Service Heads/Managers. Management responses to recommendations are included in each assignment report.			
Report Author	Piyush Fatania, Head of Audit Risk Assurance Tel: 01452 328883 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 2020/21			
Implications (details at the end of the report)	Financial	Legal	Equality	Environmental
	No	No	No	No

1.0 INTRODUCTION/BACKGROUND

1.1 Members approved the Internal Audit Plan 2020/21 at the 26th May 2020 Audit and Standards Committee meeting.

1.2 Covid-19 has placed significant pressures on Council services and has impacted (and continues to impact) the Council's priorities, objectives and risk environment. Due to the changing position and to ensure that the Risk Based Internal Audit Plan meets the assurance needs of the Council, the Revised Risk Based Internal Audit Plan 2020/21 was approved by Members at 6th October 2020 Audit and Standards Committee meeting.

1.3 In accordance with the Public Sector Internal Audit Standards (PSIAS) 2017, this report (through Appendix A) details the outcomes of Internal Audit work carried out in accordance with the approved Plan.

2.0 MAIN POINTS

2.1 The Internal Audit Activity Progress Report 2020/21 at Appendix A summarises:

- The progress against the Revised Internal Audit Plan 2020/21, including the assurance opinions on the effectiveness of risk management and control processes;
- The outcomes of the Internal Audit activity during January to March 2021; and
- Special investigations/counter fraud activity.

2.2 The report is the fourth progress report in relation to the Internal Audit Plan 2020/21. It is also the third progress report to reflect the approved 2020/21 Plan revisions (due to the impact of Covid).

2.3 As reflected within the Internal Audit Progress Report, new activities progressed by Audit Risk Assurance (ARA) since the start of the pandemic include (but are not exclusive to):

- The provision of consultancy support (from both our Internal Audit and Counter Fraud teams) to the Revenues and Benefits service and Finance regards Business Grants and Supplier Relief;
- Internal Audit review of the Lost Sales, Fees and Charges Grant (Covid 19) claims 1and 2; and
- Review of the financial close information required to support stage 2 of the Council's Ofgem Application: Non-Domestic Renewable Heat Incentive.

3.0 CONCLUSION

3.1 The purpose of this report 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.

3.2 In accordance with the PSIAS and as reflected within the Audit and Standards Committee work programme, the final Internal Audit Activity Progress Report against the approved Revised Internal Audit Plan 2020/21 is scheduled to be presented to the Audit and Standards Committee at the July 2021 meeting (specific date to be confirmed).

4.0 IMPLICATIONS

4.1 Financial Implications

There are no financial implications arising directly from this report.

Andrew Cummings – Director of Finance
Email: financial.imp@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.

Patrick Arran, Monitoring Officer
Email: patrick.arran@stroud.gov.uk

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 as a result of the recommendations made within this report.

This page is intentionally left blank

Internal Audit Activity
Progress Report
2020/21

ARA
AuditRiskAssurance

STROUD DISTRICT COUNCIL

(1) Introduction

All local authorities must make proper provision for Internal Audit in line with the 1972 Local Government Act (S151) and the Accounts and Audit Regulations 2015. The latter states that a relevant authority "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". The Internal Audit Service is provided by Audit Risk Assurance under a Shared Service agreement between Stroud District Council, Gloucester City Council and Gloucestershire County Council and carries out the work required to satisfy this legislative requirement and reports its findings and conclusions to management and to this Committee.

The guidance accompanying the Regulations recognises the Public Sector Internal Audit Standards 2017 (PSIAS) as representing "proper Internal Audit practices". The standards define the way in which the Internal Audit Service should be established and undertake its functions.

The Shared Service Internal Audit function is conducted in conformance with the International Standards for the Professional Practice of Internal Auditing.

(2) Responsibilities

Management are responsible for establishing and maintaining appropriate risk management processes, control systems (financial and non financial) and governance arrangements. Internal Audit plays a key role in providing independent assurance and advising the organisation that these arrangements are in place and operating effectively. Internal Audit is not the only source of assurance for the Council. There are a range of External Audit and inspection agencies as well as management processes which also provide assurance and these are set out in the Council's Code of Corporate Governance and its Annual Governance Statement.

(3) Purpose of this Report

One of the key requirements of the standards is that the Head of Audit Risk Assurance should provide progress reports on internal audit activity to those charged with governance. This report summarises:

- The progress against the 2020/21 Revised Internal Audit Plan, including the assurance opinions on the effectiveness of risk management and control processes;
- The outcomes of the Internal Audit activity during January to March 2021; and
- Special investigations/counter fraud activity.

(4) Progress against the 2020/21 Revised Internal Audit Plan, including the assurance opinions on risk and control

The schedule provided at **Attachment 1** provides the summary of 2020/21 audits which have not previously been reported to the Audit and Standards Committee.

The schedule provided at **Attachment 2** contains a list of all of the 2020/21 Internal Audit Plan activity undertaken during the financial year to date, which includes, where relevant, the assurance opinions on the effectiveness of risk management arrangements and control processes in place to manage those risks and the dates where a summary of the activities outcomes has been presented to the Audit and Standards Committee. Explanations of the meaning of these opinions are shown in the below table.

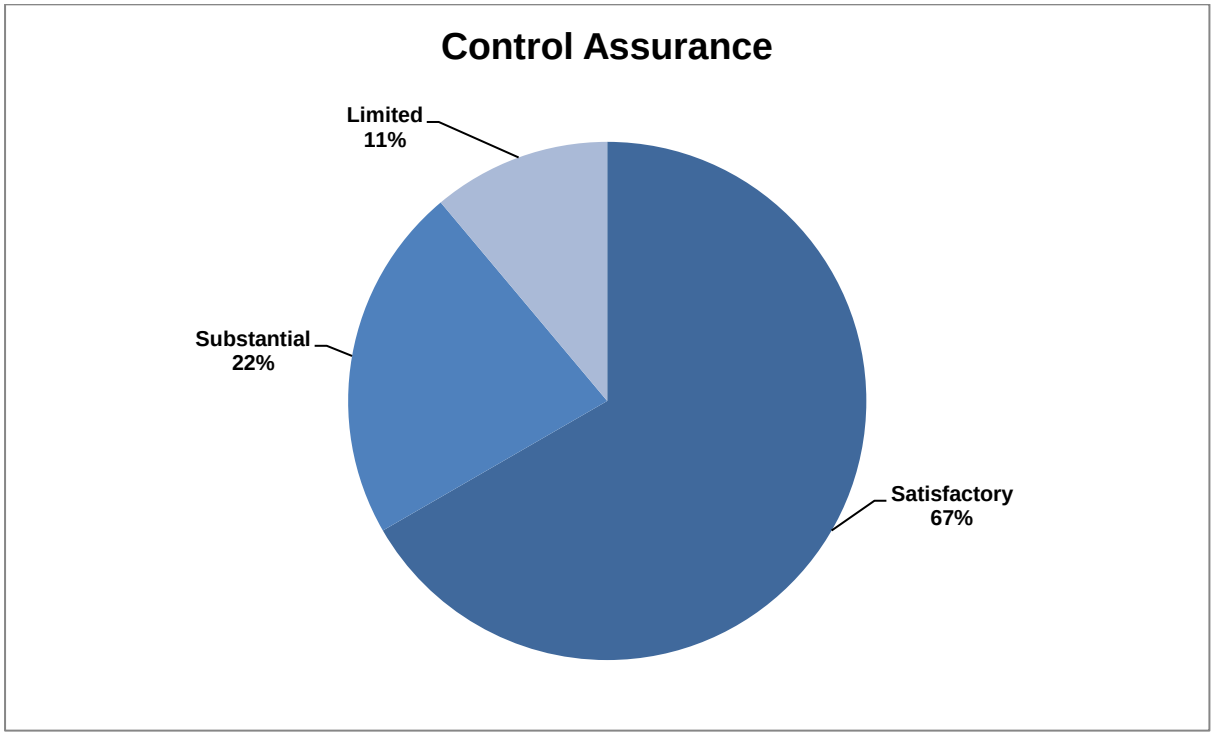
Assurance Levels	Risk Identification Maturity	Control Environment
Substantial	**Risk Managed** Service area fully aware of the risks relating to the area under review and the impact that these may have on service delivery, other service areas, finance, reputation, legal, the environment, client/customer/partners, and staff. All key risks are accurately reported and monitored in line with the Council's Risk Management Policy.	• System Adequacy – Robust framework of controls ensures that there is a high likelihood of objectives being achieved • Control Application – Controls are applied continuously or with minor lapses
Satisfactory	**Risk Aware** Service area has an awareness of the risks relating to the area under review and the impact that these may have on service delivery, other service areas, finance, reputation, legal, the environment, client/customer/partners, and staff. However some key risks are not being accurately reported and monitored in line with the Council's Risk Management Policy.	• System Adequacy – Sufficient framework of key controls for objectives to be achieved but, control framework could be stronger • Control Application – Controls are applied but with some lapses
Limited	**Risk Naïve** **Due to an absence of accurate and regular reporting and monitoring of the key risks in line with the Council's Risk Management Policy, the service area has not demonstrated a satisfactory awareness of the risks relating to the area under review and the impact that these may have on service delivery, other service areas, finance, reputation, legal, the environment, client/customer/partners and staff.**	• **System Adequacy – Risk of objectives not being achieved due to the absence of key internal controls** • **Control Application – Significant breakdown in the application of control**

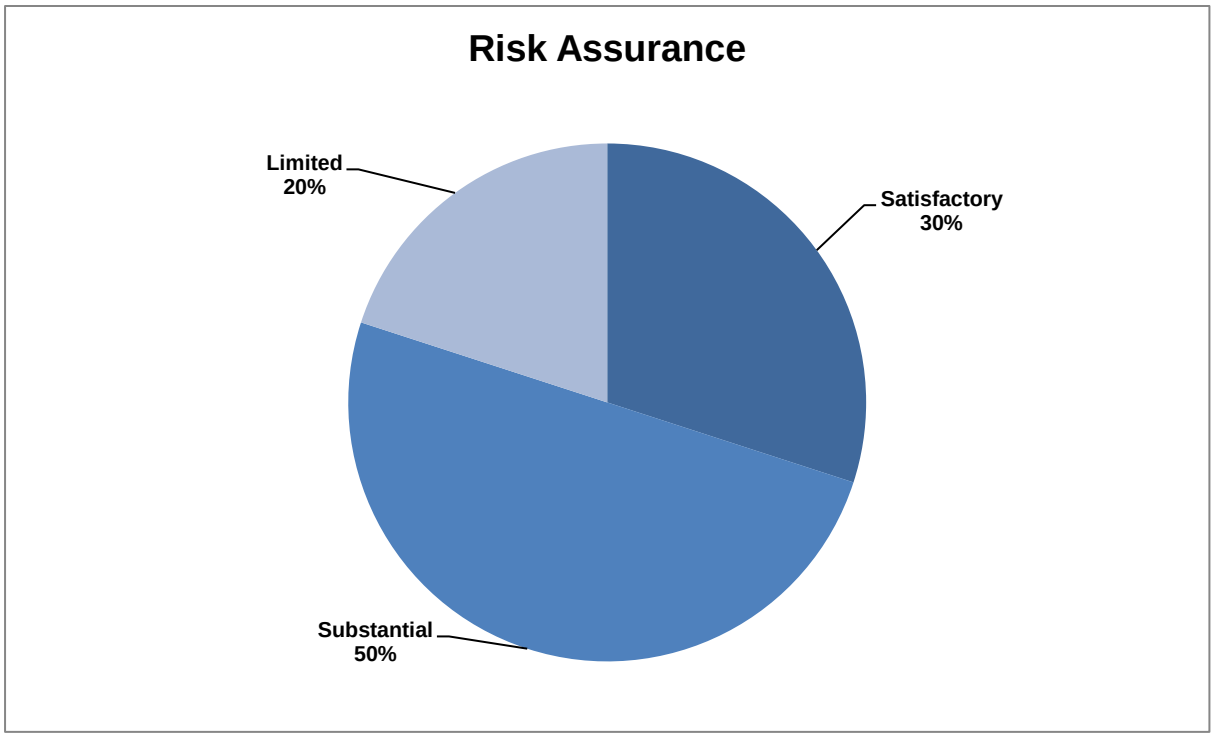
Appendix A

(4a) Summary of Internal Audit Assurance Opinions on Risk and Control

The pie charts below show the summary of the risk and control assurance opinions provided within each category of opinion i.e. substantial, satisfactory and limited in relation to the 2020/21 audit activity undertaken up to March 2021.

It is noted that the split assurance risk opinion (Limited/Satisfactory) on Tenancy Lettings reported to Committee in January 2021 has been reflected in both relevant assurance levels (limited/satisfactory) within the risk assurance pie chart.





(4b) Limited Control Assurance Opinions

Where audit activities record that a limited assurance opinion on control has been provided, the Audit and Standards Committee may request Senior Management attendance to the next meeting of the Committee to provide an update as to their actions taken to address the risks and associated recommendations identified by Internal Audit.

(4c) Audit Activity where a Limited Assurance Opinion has been provided on Control

During January to March 2021, no limited assurance opinions on control have been provided.

(4d) Satisfactory Control Assurance Opinions

Where audit activities record that a satisfactory assurance opinion on control has been provided, where recommendations have been made to reflect some improvements in control, the Committee can take assurance that improvement actions have been agreed with management to address these.

(4e) Internal Audit Recommendations

During January to March 2021, Internal Audit made a total of **4** recommendations to improve the control environment, **0** of which were high priority and **4** which were medium priority recommendations (**100%** of these being accepted by management).

The Committee can take assurance that all high priority recommendations will remain under review by Internal Audit, by obtaining regular management updates, until the required action has been fully completed.

(4f) Risk Assurance Opinions

During the period January to March 2021, no limited assurance opinions on risk have been provided on completed audits from the 2020/21 Revised Internal Audit Plan.

Monitoring of the implementation of recommendations to manage the risks identified is owned by the relevant manager(s) and helps to further embed risk management in to the day to day management, risk monitoring and reporting process.

(4g) Internal Audit Plan 2020/21 Refresh – Covid-19

Covid-19 has placed significant pressures on Council services and has impacted (and continues to impact) the Council's priorities, objectives and risk environment.

Due to this changing position and to ensure that the Risk Based Internal Audit Plan meets the assurance needs of the Council, the Internal Audit Plan 2020/21 was reviewed and refreshed in consultation with Officers (Strategic Leadership Team, Heads of Service and Service Managers). This included consideration of newly identified activities, current activities that should be prioritised within 2020/21 and activity deferrals/cancellations (due to risk).

The Revised Internal Audit Plan 2020/21 was presented to Audit and Standards Committee on 6th October 2020 and approved.

This included reflection of the new activities completed by ARA since the outcome of the pandemic. For example and as reflected within the Internal Audit Progress Report, to date within 2020/21 ARA has:

- Provided consultancy support (from both our internal audit and counter fraud teams) to the Revenues and Benefits service and Finance regards Business Grants and Supplier Relief.

- Progressed Internal Audit review of the Lost Sales, Fees and Charges Grant (Covid-19) claims 1 and 2; and

- Completed review of the financial close information required to support stage 2 of the Council's Ofgem Application: Non-Domestic Renewable Heat Incentive.

Completed Internal Audit Activity during January to March 2021

Summary of Substantial Assurance Opinions on Control

Service Area: Resources

Audit Activity: Corporate Induction Process

Background

The Council employs 456 staff, which is 324 whole time equivalents, as at 31st December 2020. The impact of Covid-19 remote working upon staff induction will result in a flexible and pragmatic approach being implemented. For the period April to December 2020, 33 new members of staff joined the Council.

A corporate induction process for staff should result in both employee and employer benefitting in terms of efficiently and effectively integrating new hires into the Council.

Scope

The audit reviewed the robustness of the Council's Corporate Staff Induction Process, to determine whether it is consistently applied.

Risk Assurance – Substantial

Control Assurance – Substantial

Key Findings

- The corporate staff induction process is directly linked to the Council's workforce plan, which seeks to ensure that suitably qualified people are recruited to ensure service continuity is delivered to the district. The continuity of services is a strategic risk, which should be frequently reviewed, assessed and recorded on the Excelsis risk and performance system.

- Audit review of Excelsis confirmed that the continuity of services risk had been reviewed by lead officers and clearly documented the mitigating actions taken to respond to the Covid-19 pandemic.

- It is essential to have a systematic documented induction process for staff in place, to facilitate successful integration and avoid the risk of applying a haphazard approach. The Intranet (HUB) was reviewed with the objective of assessing the completeness of available information and documentation for new staff. The review of the HUB for information and documents for new staff did not identify any significant weaknesses.

- When new members of staff join the Council, it is important to ensure that their IT requirements and access rights are effectively set up so that the induction process runs smoothly. A walkthrough test for a new member of staff confirmed this as being appropriately in place and actioned.

- Having an effective pre-employment process embedded from the offer stage, enables the transition for the new member of staff to be conducted effectively. A walkthrough test was completed and verified that the pre-employment process was operating correctly.

- During the initial induction period in week one, it is important to make new staff aware of the employee benefits they have and the Council's employment policies in place. Audit testing found that week one induction procedures would benefit from a refresh by particularly drawing new staff's awareness to all the employment benefits available, therefore a medium priority recommendation was made.

- The importance of completing staff induction reviews on a regular basis, informs the employee, service manager and the Human Resources (HR) team of progress, performance achievements and development needs. Audit testing of induction reviews confirmed clear documentation of the member of staff's progress, performance achievements and future development needs.

- As part of the corporate induction process, staff training comprises two elements; i) corporate; and ii) service, tailored to the needs of the role and responsibilities. Test results for a sample of three confirmed that new staff received appropriate training.

- Effective HR monitoring controls for corporate employee induction ensures that the team are correctly overseeing the actual process in place for staff. Monitoring controls reviewed for a sample of three new staff, verified that they were working effectively.

Conclusion

Internal Audit's review of the Council's Corporate Staff Induction Process, found that it had been consistently applied for the selected sample of new employees. The process was found to be comprehensive and the embedded systematic approach reflected an appropriate and effective control environment.

One audit recommendation has been raised regards the contents of the week one induction, to ensure that the staff benefits available are adequately signposted and the new employee confirms that they have received all relevant guidance and information.

Management Actions

Management have responded positively to the one recommendation and it has been promptly implemented by the Council.

Summary of Satisfactory Assurance Opinions on Control

Service Area: Place

Audit Activity: Gloucestershire Building Control Partnership (GBCP) - Limited Assurance Follow Up

Background

Stroud District Council (SDC) and Gloucester City Council (GCityC) have collaborated to provide a shared local government building control service known as the Gloucestershire Building Control Partnership (GBCP). The GBCP was established on 1st July 2015 through a Section 101 Agreement, with staff being employed by SDC acting as the host Authority. The Building Control function comprises of two elements:

- Plan vetting and inspection of applications, which is a statutory Council function in direct competition with the private sector; and
- Enforcement of Building Control legislation and regulations.

A review of this activity was undertaken during 2019/20. The audit concluded that only 'Limited Assurance' could be provided for both the risk identification maturity and the control environment.

Scope

This follow up audit review sought to provide assurance that the recommendations raised in the 2019/20 audit review have been fully implemented or there is an approved action plan to show how and when they will be implemented.

Risk Assurance – Substantial

Control Assurance – Satisfactory

Key Findings

The status of the four high and five medium priority recommendations raised in the 2019/20 audit at the point of this Internal Audit follow up review is summarised in the table below:

Original Recommendation Priority	Original Recommendations Raised	Position at 2020/21 Internal Audit Follow Up	
		Implemented	Partially Implemented
High Priority	4	3	1
Medium Priority	5	5	

As result of the current health pandemic, GBCP has had to adapt to a new way of working resulting in:

- A change in its work priorities;
- A focus on maintaining service continuity;
- The revaluation of the requirements and implications required to maintain the service in a new environment; and
- The management and wellbeing of officers.

It is therefore commendable that GBCP management have fully implemented eight out of the nine original audit recommendations and that GBCP are progressing resolution of the one outstanding recommendation. Details of the partially completed recommendation are:

- High Priority recommendation one – Review and amendment of the Section 101 Agreement.

  A review of the Section 101 Agreement was undertaken by the SDC Building Control Manager during 2019/20 and variations to this agreement were submitted to and approved by the September 2020 GBCP Shared Service Board. A review, by Internal Audit, of the key requirements of the Section 101 Agreement and any subsequent variations for compliance with them highlighted, that due to the impact of the Covid-19 pandemic, the following requirements have not been fully completed as at the time of this follow up review:

  - Production of two additional progress reports for April and July;
  - Production of GBCP minutes within stated timeframes;
  - Formal agreement of the Service Delivery Plan / Business Plan by the stated timeframe;
  - Application of Department for Communities and Local Government (DCLG) performance standards;
  - Development of a customer feedback procedure; and

- Completion and approval of a five year financial plan.

The SDC Building Control Manager is fully aware of the above areas and is managing them to ensure compliance during the first half of 2021/22.

A summary of the eight completed recommendations are as follows:

High Priority recommendations

- SDC Shared Service Board members, at the point of this follow up review, have demonstrated an active role in the GBCP;
- The trading account reserve balance, building control fees and the forecast of future income and expenditure was reviewed by the Board and appropriate actions agreed; and
- The financial statement for the financial years 2017/18 to 2019/20 were published on the GBCP website.

Medium Priority recommendations

- Building Control officers have completed a timesheet on an agreed regular basis to either reaffirm the current apportionment between chargeable and non-chargeable services or to adjust the calculation;
- A review of the basis for apportioning costs for the 'non-trading' account between SDC and GCityC was undertaken by the Board;
- The data owner for the Building Control systems was agreed by the Board;
- Monthly income reconciliations have been completed for the period April to September 2020 and subject to SDC Building Control Manager review; and
- The debt recovery process was approved by the Board.

Conclusion

Good progress has been made by management in implementing Internal Audit's agreed recommendations from the 2019/20 audit review, particularly in the current unprecedented work environment due to the Covid-19 pandemic.

Management Actions

The actions taken by GBCP to implement the recommendations have resulted in a strengthening of the control environment. One recommendation remains in progress at the point of audit follow up, for implementation in early 2021/22.No new recommendations have been raised as a result of the audit follow up review.

Service Area: Resources

Audit Activity: Littlecombe Scheme - Limited Assurance Follow Up

Background

The Littlecombe development is a mixed-use regeneration scheme providing 600 new homes, community facilities and other commercial opportunities. The Council took ownership of the site from the South West Regional Development Agency in 2011 for £1. The intention was to unlock a stalled scheme for the benefit of Dursley, Cam and district.

The Council stepped into the partnership agreement with a national property development company and is entitled to 85% of the net development profit at completion of the scheme (July 2023), although this potential financial gain is subsidiary to the main purpose of leading the scheme to completion.

A review of this activity was undertaken during 2019/20. The audit concluded that only 'Limited Assurance' could be provided for both the risk identification maturity and the control environment.

Scope

This audit sought to provide assurance that the recommendations raised in the 2019/20 audit review had been fully implemented or there was an approved action plan to show how and when they would be implemented.

Risk Assurance – Substantial

Control Assurance – Satisfactory

Key Findings

The status of the six original (2019/20) audit recommendations at the point of this Internal Audit follow up review is summarised in the table below:

Original Recommendation Priority	Original Recommendations Raised	Position at 2020/21 Internal Audit Follow Up	
		Implemented	Partially Implemented
High Priority	4	3	1
Medium Priority	2	2	

Details of the partially completed recommendation are as follows:

- High Priority recommendation one – Develop and introduce an appropriate governance and reporting structure.

The governance arrangements for the Littlecombe scheme and the reporting structure was determined by Property Services and documented in the Council's corporate risk and performance management system (Excelsis). This consisted of the Investment and Development Panel and one to one meetings between the Property Manager and Principal Estates Surveyor, and Head of Property Services and Property Manager to discuss and manage the Littlecombe scheme.

Due to the pandemic impact, the Investment and Development Panel has not met during 2020. The purpose and scope of this panel is also being evaluated by the Strategic Director of Place. Verbal assurance from the Property Manager was received by Internal Audit that the one to one meetings have taken place and the Littlecombe scheme discussed, but that formal notes of these meetings have not been retained.

An 'Information Sheet' on the progress and current position of the Littlecombe scheme is planned to be written by Property Services during the first half of 2021 and presented to Members. It will then be published on the Council's website for residents so that all are apprised of the development. Going forward an 'Information Sheet' is expected to be published annually thereafter.

The five completed recommendations were relevant to the following areas:

- Regular review of the scheme strategic and operational risks, including documentation on Excelsis and confirmation of risk appetite;
- Receipt and review of the completed Project Expenditure Accounts from the developer in the frequency as detailed in the Development Agreement; and
- Project Expenditure Accounts to include assertions that they represent a true and fair view and these are verified by the developer lead Finance Officer.

Conclusion

Good progress has been made by management in implementing Internal Audit's agreed recommendations from the 2019/20 audit review, particularly in this unprecedented environment we are all working under due to the Covid-19 pandemic.

Management Actions

The actions taken by management to implement the recommendations have resulted in a strengthening of the control environment. One recommendation remains in progress at the point of audit follow up, for implementation in 2021/22.No new recommendations have been raised as a result of the audit follow up review.

Appendix A – Attachment 1

Summary of Consulting Activity, Grant Certification and/or Support Delivered where no Opinions are provided

Service Area: Resources (Grant Certification)

Audit Activity: Lost Sales, Fees and Charges Grant Claim 1 and 2

Background

Covid-19 has impacted local authorities' ability to generate revenues in several service areas as a result of lockdown, government restrictions and social distancing measures related to the pandemic. This new, one-off income loss scheme (the scheme) will compensate for irrecoverable and unavoidable losses from sales, fees and charges income generated in the delivery of services in the financial year 2020/21.

The scheme involves a 5% deductible rate, whereby authorities absorb losses on 5% of their planned 2020/21 sales, fees and charges income, with government compensating them for 75p in every pound of relevant loss thereafter.

The grant scheme is co-ordinated by the Ministry of Housing, Communities and Local Government (MHCLG), and is submitted in three claims covering four consecutive calendar months each.

The scheme also requires a reconciliation process to be completed by the Council after the submission of the third claim and is due to account for losses claimed for in the early part of the scheme that may ultimately be recoverable, and others that might ultimately be irrecoverable when recoverability was originally considered possible.

Scope

The objective of this audit was to review the two grant submissions and supporting documentation for the period April to November 2020 (claim 1 – April to July 2020 and claim 2 – August to November 2020), with the objective of assessing compliance with the guidance issued by MHCLG.

Key Findings

The grant claim for April 2020 to July 2020 totalled £512,963. The grant claim for August 2020 to November 2020, totalled £333,000.

The claims and supporting documentation/audit trail were reviewed and it was confirmed that:

- All 2020/21 budget financial values for service income had been correctly recorded on the grant claims as documented in the Council's Financial Management System;
- The net losses for the period April to November 2020 matched to the information within the Council's Financial Management System and had been calculated correctly in accordance with the guidance issued by MHCLG;
- The parameters set out in the formula for the scheme have been correctly applied to the applicable losses claimed for in the period (April 2020 to November 2020);
- MHCLG accepted grant claim 1 and promptly paid £512,963 on 27th November 2020; and
- As at 1st March 2021, MHCLG are due to settle the second grant claim for £333,000 shortly.

Conclusion

Internal Audit can confirm that compilation of the Lost Sales, Fees and Charges grant claims for the period April to November 2020 complied with the guidance issued by MHCLG.

Management Actions

Not applicable – no audit recommendations raised.

Service Area: Communities

Audit Activity: Housing Reactive Repairs and Maintenance - Property Care Operations Manual

Background

The Property Care Manual has been developed to ensure that the Council meets its legal obligations to repair and maintain Council owned properties; and to protect the health, safety and well-being of customers and visitors to these tenancies. A well documented procedures manual also provides clarity of agreed processes; aims to minimise the risk of errors/mistakes, and should aid employee efficiency.

The Property Care Manual currently has one section the contents are:

i) Procedures for customers to report the need for repairs;

ii) Processes for staff or contractors, to complete the repairs to the required quality standards; and

iii) Complete timely repairs to the satisfaction of the customer.

The intention is to expand this manual so it becomes a comprehensive record of the existing processes, procedures and controls for emergency and reactive repairs.

Scope

The consultancy review inspected the Property Care Operations Manual with the objective of designing out inherent known risks, and identifying any gaps within the documented control environment.

Key Findings

- The approach used to review the above manual considered the following qualities: evidence of a systematic “end-to-end” approach for the documented processes; and consistency with the reporting a repair process as documented on the Council’s website.

- Review of the above manual confirmed that substantially the existing processes, procedures and controls are suitably documented. Improvements can be made to documenting section one of the manual. In particular, improvements relating to; i) version control; ii) reporting a repair; iii) raising a repairs order; iv) appointing and scheduling; v) cancellation via engineer; vi) materials returns and credit note; vii) van stock replenishment; viii) van stock weekly audit; ix) lone worker escalation process; and x) appendices.

- Consideration has also been given to identify associated processes which have a direct correlation to the emergency and reactive repairs work streams, with the objective of enhancing the completeness of the Property Care Operations Manual and its value to staff and contractors.

- The existing Covid-19 risk assessments and health and safety procedures produced by Housing Services and details of the outside of normal working hours third party contractor would be a welcome addition to section two of the manual.

- Internal Audit acknowledges that the impact of Covid-19 will have a subsequent impact upon staff’s roles and priorities. Inspection of the Housing Repairs and Planned Maintenance Policy 2017 found that the review period of September 2020 has now lapsed, and is in need of a procedure which will update the document ready for the Housing Committee to consider for approval.

Conclusion

Review of the Property Care Operations Manual established that the repair processes are fundamentally documented. Two recommendations to improve the completeness of the manual have been made.

In addition due to its inter-relationship with the Property Care Operations Manual, one recommendation for review of the Housing Repairs and Planned Maintenance Policy in 2021 has been made to ensure that it remains fit for purpose and is subject to appropriate scrutiny and subsequent approval.

Management Actions

Management have responded positively to the three recommendations made and the proposed target date is set for these to be fully implemented by 31st August 2021.

Service Area: Communities

Audit Activity: Housing Revenue Account (HRA) Delivery Plan

Background

The Council's HRA Delivery Plan sets out the Council's direction and priority for the Council's Housing Service - enabling it to focus on the delivery of stated priorities, manage and respond to business risks and opportunities, and have appropriate contingencies in place.

The HRA Delivery Plan includes an action plan which is revised annually to ensure that it remains relevant and supports the Council's ability to meet local needs, statutory and regulatory responsibility, borrowing and debt repayment commitments, stock investment and management objectives (decent homes), service delivery, (tenancy management, resident involvement, satisfaction levels) objectives, as well as ensuring that it remains sustainable.

Following a period of consultation during summer 2019 with tenants and leaseholders and the application of the Tenant survey reports (STAR Survey), members of Housing Committee and the Housing Review panel reviewed and updated the HRA Delivery Plan 2020-2025 with additional strategic priorities. This was approved by the Housing Committee on 10th December 2019.

The HRA Delivery Plan was updated with the following key strategic objectives for the medium term:

- Improve tenant satisfaction and culture exploring different avenues and opportunities to build, enhance and grow communities;
- Delivery of the older person's strategy and action plan over the next 5 years including the current programme to modernise the Council's sheltered housing stock and the quality of the 'housing offer';
- New development;
- Investment in sustainable and attractive estates and stock; and
- Implementation of the updated energy strategy.

Scope

The review sought to determine whether the updated action plan would effectively address the key strategic objectives defined within the HRA Delivery Plan 2020-2025. The specific objectives of the review were to provide assurance on the following areas:

a) The HRA Delivery Plan 2020-2025 action plan documents activities that will address each of the five key strategic objectives;

b) Each action is specific, measurable, achievable, realistic, time-bound with responsible officers assigned to manage the action; and

c) Effective monitoring arrangements are in place to track that actions are progressing as planned, and in line with the agreed target dates.

Position Statement

Due to the challenges of Covid-19 and lockdown periods, Stroud District Council priorities have had to shift dramatically to support communities, residents and businesses. This has meant that the strategic objectives defined within the HRA Delivery Plan have been impacted as it has not been possible to conduct the required consultations, and work streams that were planned have either been suspended or deferred until lockdown measures are eased.

To support the Head of Housing Services at this challenging time, Internal Audit has adopted an agile audit approach to delivering the audit objectives and to ensure that the audit provides added value to the Council and Head of Housing Services.

As audit testing for objectives a) and b) would not have been appropriate due to the impact of Covid-19 on Tenant Services, this position statement has been written to update Members and confirm that it is internal audit's intention to undertake a full review during 2021/22.

Progress update for objective c): Effective monitoring arrangements are in place to track that actions are progressing as planned, and in line with the agreed target dates.

Internal Audit can confirm that in July 2020, the Head of Housing Services provided members with an Information Sheet update regarding the Housing Revenue Account Delivery Plan 2020-2025. This Information Sheet was also referenced in the agenda pack for the Housing Committee meeting on 22nd September 2020.

Internal Audit has established:

- The HRA Delivery Plan 'Action Plan' is a living document with clear measures of success and targets dates;
- The HRA Delivery Plan 'Action Plan' is maintained and reviewed regularly by the Head of Housing Services; and
- The Head of Housing Services, Head of Housing Contracts, New Homes and Regeneration Manager and the Head of Strategic Housing Services are aware of the 'Action Plan' and provide updates to it.

Next Steps

The Head of Housing Services will continue to work with the action plan leads to progress the HRA Delivery Plan 'Action Plan' and continue to annually update the Housing Committee.

A full HRA Delivery Plan internal audit is proposed for completion within the draft Internal Audit Plan 2021/22.

Summary of Special Investigations/Counter Fraud Activities

Current Status

The Counter Fraud Team (CFT) within Internal Audit has received five actionable referrals in 2020/21 to date, three of which have been closed and previously reported to the Audit and Standards Committee.

The two remaining ongoing cases are both Covid-19 grant related and will be reported on further once closed.

In addition to the referrals that require further investigation, the CFT has continued to provided support and guidance to the Council in respect of the government initiative Coronavirus: Small Business Grant Fund (SBGF) as requested. Since the start of the Covid-19 pandemic, ARA has also provided the Council with regular updates on local and national scams which sought to take advantage of the unprecedented circumstances, including a rise in bank mandate frauds, inflated claims, duplicate payments and the submission of fraudulent SBGF applications.

Any fraud alerts received by Internal Audit from National Anti-Fraud Network (NAFN) and other credible organisations are passed onto the relevant service areas within the Council, to alert staff to the potential fraud.

National Fraud Initiative (NFI)

Internal Audit continues to support the NFI which is a biennial data matching exercise administered by the Cabinet Office. The data collections for the 2021/22 exercise have been uploaded to the Cabinet Office. The release of the data matches began in mid January 2021 and staff have been advised that the matches are now ready for review. The timetable can be found using the following link GOV.UK.

Examples of data sets include housing, insurance, payroll, creditors, council tax, electoral register and licences for market trader/operator, taxi drivers and personal licences to supply alcohol. 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.

It is understood that the Counter Fraud Unit (hosted by Cotswold District Council) will be undertaking some of the match reviews on behalf of the Council and the Counter Fraud Unit findings will be reported to the Audit and Standards Committee separately.

ARA Audit Risk Assurance

Progress Report including Assurance Opinions

Department	Activity Name	Priority	Activity Status	Risk Opinion	Control Opinion	Reported to Audit and Standards Committee	Comments
Council Wide	Local Government Association Peer Review	1	Planned				Brought Forward from 19/20 plan. Interim report confirming 19/20 position issued to Committee in July 20. Audit review to be concluded and reported in 20/21 annual report.
Council Wide	Risk and Performance Reporting	1	Deferred				Activity proposed for deferral through the draft Internal Audit Plan 21/22. Activity scope updated based on consultation and risk assessment.
Council Wide	Supplier Relief	1	Consultancy				**New Activity.** To be reported in 20/21 annual report.
Change and Transformation	Modernisation Programme	1	Planned				Brought Forward from 19/20 plan.
Place	Brimscombe Port - Project Management	1	Final Report Issued	Substantial	Satisfactory	06/10/2020	
Place	Carbon Neutral - Strategy	1	Deferred				Activity proposed for deferral through the draft Internal Audit Plan 21/22 (Covid 19 impact).
Place	Gloucestershire Building Control Partnership - Limited Assurance Follow Up	1	Final Report Issued	Substantial	Satisfactory	27/04/2021	
Place	Planning Applications	1	Audit in Progress				Brought Forward from 19/20 plan.
Place	Covid 19 Recovery Strategy	1	Audit in Progress				**New Activity.** Work replaces Corporate Delivery Plan audit.
Resources	Constitution Review	1	Deferred				Deferral (due to work on Business Grants) approved via the Revised Internal Audit Plan 20/21. Re-considered as part of 21/22 audit planning process.
Resources	Corporate Delivery Plan	1	Deferred				Deferral (replaced by Covid 19 Recovery Strategy audit) approved via the Revised Internal Audit Plan 20/21. Re-considered as part of 21/22 audit planning process.
Resources	Corporate Induction Process	1	Final Report Issued	Substantial	Substantial	27/04/2021	
Resources	ICT Action Plan	1	Final Report Issued	Satisfactory	Satisfactory	06/10/2020	Brought Forward from 19/20 plan.
Resources	ICT Service Desk	1	Consultancy				To be reported in 20/21 annual report.
Resources	IT Disaster Recovery	1	Draft Report Issued				Consultancy. To be reported in 20/21 annual report.
Resources	Cyber Security	1	Audit in Progress				To be reported in 20/21 annual report.
Resources	IT Infrastructure Strategy	1	Deferred				Activity proposed for deferral through the draft Internal Audit Plan 21/22 (Covid 19 impact).
Resources	Information Management (Data Breaches)	1	Audit in Progress				
Resources	Littlecombe Scheme - Limited Assurance Follow Up	1	Final Report Issued	Substantial	Satisfactory	27/04/2021	
Resources	Payroll - Starters	1	Final Report Issued	Substantial	Substantial	06/10/2020	
Resources	Procurement	1	Draft Report Issued				To be reported in 20/21 annual report.
Resources	Ofgem Application: Non-Domestic Renewable Heat Incentive	1	Final Report Issued	Not applicable	Not applicable	26/01/2021	**New Activity.**
Resources	Lost Sales Fees and Charges - claim 1	1	Final Report Issued	Not applicable	Not applicable	27/04/2021	**New Activity.** Outcomes from claims 1 and 2 consolidated in to one summary paragraph.
Resources	Lost Sales Fees and Charges - claim 2	1	Final Report Issued	Not applicable	Not applicable	27/04/2021	**New Activity.** Outcomes from claims 1 and 2 consolidated in to one summary paragraph.
Communities	HRA Delivery Plan	1	Final Report Issued	Not Applicable	Not Applicable	27/04/2021	Position Statement reported to April 21 Audit & Standards Committee. New activity (updated scope) also proposed through the draft Internal Audit Plan 21/22.
Communities	Anti-social Behaviour Management	2	Deferred				Deferral due to work on the priority 1 Covid-19 relevant new activities (e.g. Business Grants and Lost Sales Fees and Charges). Re-considered as part of 21/22 audit planning process.
Communities	Careline Service	2	Deferred				Deferral due to work on the priority 1 Covid-19 relevant new activities (e.g. Business Grants and Lost Sales Fees and Charges). Re-considered as part of 21/22 audit planning process.
Communities	Complaints Handling	2	Final Report Issued	Satisfactory	Satisfactory	06/10/2020	Brought Forward from 19/20 plan.
Communities	Housing Benefits - Overpayments	2	Deferred				Deferral (due to work on Business Grants) approved via the Revised Internal Audit Plan 20/21. Re-considered as part of 21/22 audit planning process.
Communities	Tenancy Lettings	2	Final Report Issued	Limited/Satisfactory	Satisfactory	26/01/2021	Split opinion on risk identification maturity - Limited/Satisfactory.
Communities	Electrical Works Contract	1	Final Report Issued	Limited	Limited	17/11/2020	
Communities	Housing Reactive Repairs & Maintenance - Property Care Operations Manual	1	Final Report Issued	Not applicable	Not Applicable	27/04/2021	
Communities	Stratford Park Leisure Centre	1	Audit in Progress				**New Activity.**

Progress Report including Assurance Opinions

Department	Activity Name	Priority	Activity Status	Risk Opinion	Control Opinion	Reported to Audit and Standards Committee	Comments
Communities	Business Grants	1	Consultancy				**New Activity.** To be reported in 20/21 annual report.
Communities	Youth Service	2	Deferred				Deferral (due to work on Business Grants) approved via the Revised Internal Audit Plan 20/21. Re-considered as part of 21/22 audit planning process.

STROUD DISTRICT COUNCIL **AGENDA ITEM NO**

AUDIT AND STANDARDS COMMITTEE

27 APRIL 2021 **7**

Report Title	**DRAFT INTERNAL AUDIT PLAN 2021/22**
Purpose of Report	To provide the Committee with a summary of the draft Risk Based Internal Audit Plan 2021/22 as required by the Accounts and Audit Regulations 2015 and the Public Sector Internal Audit Standards (PSIAS) 2017.
Decision(s)	**The Audit and Standards Committee RESOLVES to:** **a) Agree that the Annual Risk Based Internal Audit Plan 2021/22 reflects the current risk profile of the Council; and** **b) Approve the Annual Risk Based Internal Audit Plan 2021/22 as detailed in Appendix A.**
Consultation and Feedback	Officers (Senior Leadership Team, Heads of Service and Service Managers); Members (via the Audit and Standards Committee Risk Based Audit Planning workshop on 26th January 2021); and External Audit have been consulted on the draft Annual Risk Based Internal Plan 2021/22. 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. The timing of audit work will be planned in conjunction with the appropriate managers to minimise abortive work and time.
Report Author	Piyush Fatania, Head of Audit Risk Assurance Tel: 01452 328883 Email: piyush.fatania@gloucestershire.gov.uk
Options	No other options can be considered as a Risk Based Internal Audit Plan is required by the PSIAS. The lack of such a Plan would lead to non compliance with these Standards.
Background Papers	N/A – links to legislation are in the body of the report.
Appendices	Appendix A – Draft Internal Audit Plan 2021/22

Implications (details at the end of the report)	Financial	Legal	Equality	Environmental
	No	No	No	No

1.0 INTRODUCTION/BACKGROUND

1.1 All local authorities must make proper provision for Internal Audit in line with the Accounts and Audit Regulations 2015. The Regulations provide that a relevant authority "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". Undertaking annual internal audits 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 recognises the Public Sector Internal Audit Standards (PSIAS) 2017 as representing "proper Internal Audit practices". The Standards define the way in which the Internal Audit Service should be established and undertake its functions. These Standards require the Head of Audit Risk Assurance to produce an Annual Risk Based Internal Audit Plan to determine the priorities of the Internal Audit activity. The proposed activity should be consistent with the organisation's priorities and objectives, taking into account the organisation's risk management framework, including risk appetite levels set by management and Internal Audit's own judgement of risks.

1.3 To ensure our Internal Audit resources continue to be focussed accordingly, particularly during periods of organisational change, it is essential that the Internal Audit Service understand our clients' needs, which means building relationships with key stakeholders, including other assurance/challenge providers, in order to gain crucial insight and ongoing 'intelligence' into the strategic and operational change agendas within our organisation.

1.4 This insight is not only identified at the initial development stages of the plan. Dialogue continues throughout the financial year(s) which 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 therefore needs to be dynamic and should be flexible to meet these needs.

2.0 MAIN POINTS

2.1 To ensure that an effective plan is developed, in addition to including activity requested by the Audit and Standards Committee at the Risk Based Audit Planning workshop held on 26th January 2021 and alongside Internal Audit's own assessment of risk, a consultation process took place with Senior Leadership Team, Heads of Service and Service Managers to establish priorities and assurance requirements. The proposed activity from all sources

was collated and matched against the Internal Audit resources available and prioritised accordingly.

2.2 The Audit Plan is stated in terms of estimated days input to the Council of 463 audit days, which is comparable to 2020/21. By continuing to apply risk based internal audit planning principles; this level of input, with the ability to commission Internal Audit resources from current audit framework agreements as required, is considered acceptable to provide the assurance the Council needs.

2.3 The Head of Audit Risk Assurance will continue to reassess Internal Audit resources required against the Council's priorities and risks and will amend the Plan throughout the year as required, reporting any key changes to the Audit and Standards Committee. Any additional activity required above the core provision will be agreed upfront with the S151 Officer. This approach will appropriately consider the Council's priorities and risk changes that occur due to Covid-19, ensuring that the Risk Based Internal Audit Plan remains flexible and dynamic within 2021/22.

3.0 CONCLUSION

3.1 The PSIAS requires the Head of Audit Risk Assurance to produce an Annual Risk Based Internal Audit Plan and for this Plan to be approved 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 approved 2021/22 Annual Risk Based Internal Audit Plan and any significant control issues identified will be presented to the Audit and Standards Committee.

4.0 IMPLICATIONS

4.1 Financial Implications

There are no financial implications arising directly from this report.

Andrew Cummings – Strategic Director of Resources
Tel: 01453 754115
Email: andrew.cummings@stroud.gov.uk

Risk Assessment:
Failure to deliver effective governance will negatively impact on the achievement of the Council's objectives and priorities and reputation.

4.2 Legal Implications

There are no specific legal implications in addition to those mentioned in the report.

Patrick Arran, Monitoring Officer
Tel: 01453 754369
Email: patrick.arran@stroud.gov.uk

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 as a result of the recommendations made within this report.

Draft Internal Audit Plan 2021/22

STROUD DISTRICT COUNCIL

ARA Audit Risk Assurance

Gloucester City Council · Stroud District Council · Gloucestershire County Council

Background

All local authorities must make proper provision for Internal Audit in line with the Accounts and Audit Regulations 2015 (the Regulations). These state that authorities 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'.

The guidance accompanying the Regulations recognises both the Public Sector Internal Audit Standards (PSIAS) 2017 and the Chartered Institute for Public Finance Accountants (CIPFA) Local Government Application Note for the UK PSIAS as representing 'public sector internal audit standards'. The standards define the way in which the Internal Audit Service should be established and undertake its functions.

The standards also require that an opinion is given on the overall adequacy and effectiveness of the Council's control environment comprising risk management, control and governance, which is informed by the work undertaken by the Service.

The Internal Audit service provided by Audit, Risk and Assurance (ARA) conforms to the International Standards for the Professional Practice of Internal Auditing.

What is Internal Auditing?

The role of Internal Audit is to provide independent, objective assurance to management that key risks are being managed effectively.

To do this, Internal Audit will evaluate the quality of risk management processes, systems of internal control and corporate governance frameworks, across all parts of an organisation, and to provide an opinion on the effectiveness of these arrangements. As well as providing assurance, Internal Audit's knowledge of the management of risk enables them to act as a consultant and provide support for improvement in an organisation's procedures. For example, at the development stage of a major new system where Internal Audit can help management to ensure that risks are clearly identified and appropriate controls put in place to manage them.

Why is assurance important?

By reporting to senior management that important risks have been evaluated and highlighting where improvements are necessary, Internal Audit helps senior management to demonstrate that they are managing the organisation effectively on behalf of their stakeholders. Hence Internal Audit, along with senior management and external audit, is a critical part of the governance arrangements of the Council and our work significantly contributes to the statutory Annual Governance Statement (AGS).

Development of the 2021/22 Internal Audit Plan

To enable the above, the Head of ARA is required to produce an Annual Risk Based Internal Audit Plan to determine the priorities of the Internal Audit service. The proposed activity should be consistent with the Council's priorities and objectives and take into account the risk management framework, risk appetite levels set by management and Internal Audit's own judgement of risks.

How did we develop the plan - Risk Based Internal Audit Planning (RBIAP)

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

This insight is not only identified at the initial development stages of the plan but dialogue continues throughout the financial year(s) which 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.

How did we achieve the above?

To ensure that an effective plan is developed, and alongside Internal Audit's own assessment of risk, a consultation process took place with the Audit and Standards Committee, Senior Leadership Team, Heads of Service and Service Managers to establish priorities. The proposed activity from all sources was collated and matched against the internal audit resources available and prioritised accordingly.

A flexible audit plan - Risk and Control Assurance Programme

The Audit Plan is stated in terms of estimated days input to the Council of **463** audit days, which is comparable to last year.

By continuing to apply RBIAP principles, this level of input (combined with the ability to commission Internal Audit resources from current audit framework agreements as required) is considered acceptable to provide the assurance the Council needs.

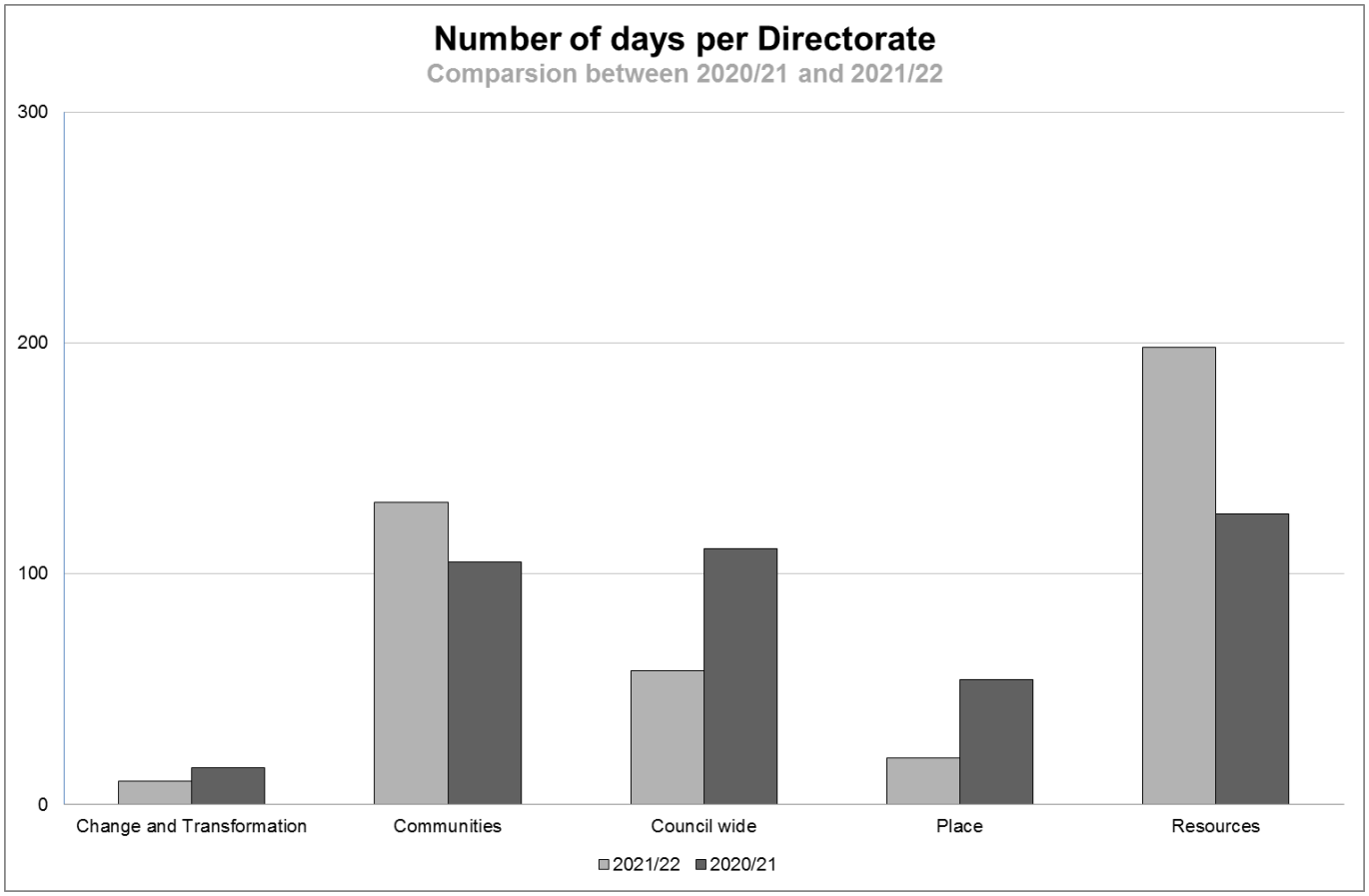
We continuously reassess resource requirements against the Council's priorities, in year demand and risks and will amend the plan throughout the year as required, reporting any key changes to the Audit and Standards Committee.

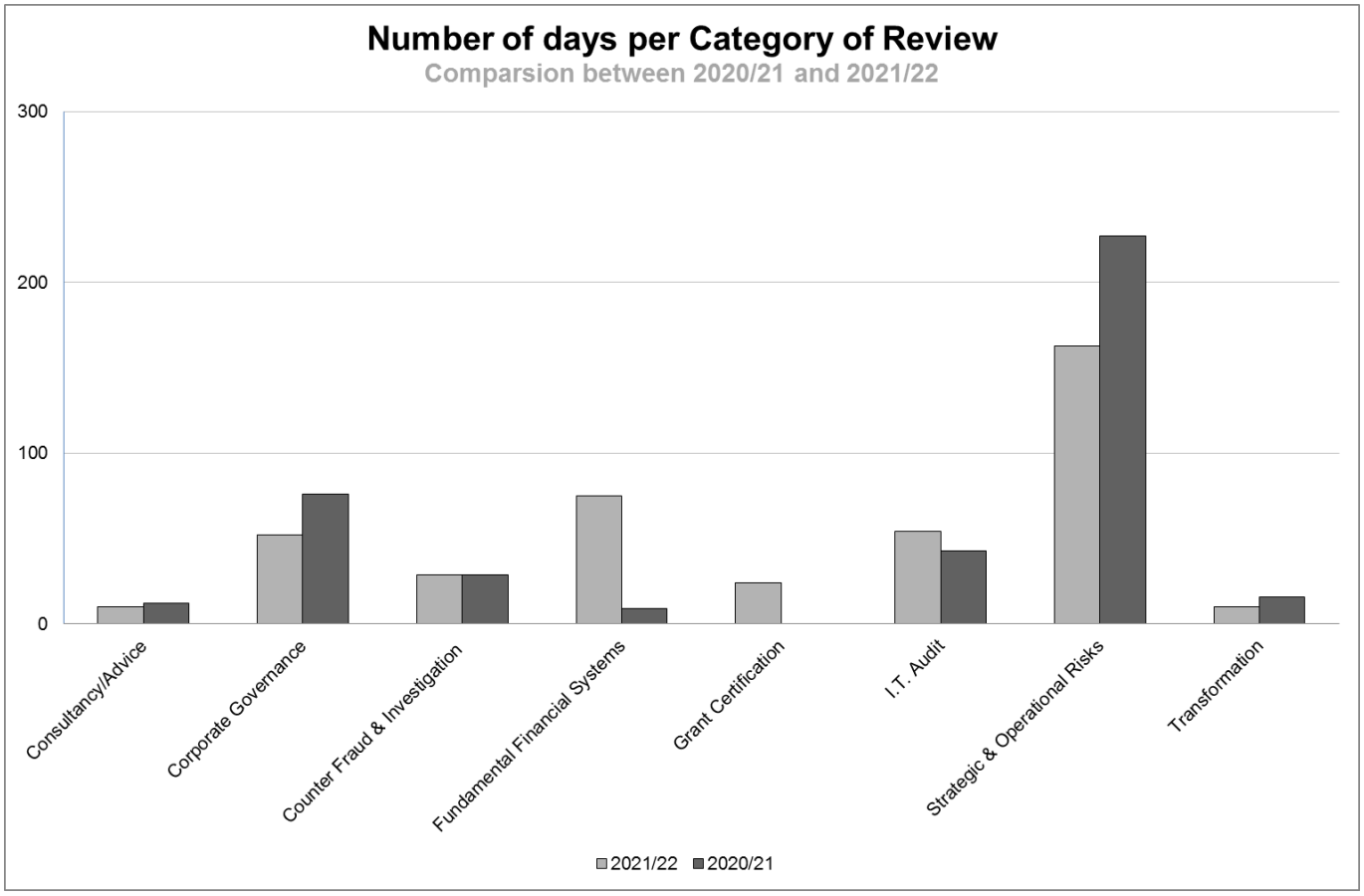
Overview of Internal Audit's Risk and Control Assurance Programme

In order to provide a high level overview of the proposed Risk and Control Assurance Programme, the charts below highlight the allocation of audit resources for the 2021/22 draft Internal Audit Plan against the original 2020/21 Internal Audit Plan for:

- Functional service area (by Directorate); and
- Category of review.

The charts exclude time allocated for management activities e.g. Committee report compilation; Committee attendance and other.


Number of days per Directorate
Comparsion between 2020/21 and 2021/22
300
200
100
0
Change and Transformation
Communities
Council wide
Place
Resources
2021/22
2020/21


Number of days per Category of Review
Comparsion between 2020/21 and 2021/22
300
200
100
0
Consultancy/Advice
Corporate Governance
Counter Fraud & Investigation
Fundamental Financial Systems
Grant Certification
I.T. Audit
Strategic & Operational Risks
Transformation
2021/22
2020/21

The key points to note within the proposals are:

- The split between each of the functional service and Council wide areas is based on risk assessment to enable the provision of the Head of ARA's annual audit opinion. The Council has reviewed and re-allocated services per Directorate/function within the last year. The 2021/22 plan columns reflecting the current position of each function/activity (e.g. Council Tax is within Resources in 2021/22, however has previously come under Communities);
- Grant certification/review assurance (both Covid-19 and other funding streams) required within 2021/22 is captured under Resources;
- Continued focus on corporate governance and strategic and operational risks (including relevant Covid-19 risk themes);
- Increased emphasis on providing assurance that the Council's fundamental financial systems are being effectively managed, following reduced focus on this area in the 2020/21 original plan;
- Continued focus on ICT risks and counter fraud activity, which includes the use of Data Analytics to help support more efficient and effective internal audit practices;
- Undertaking follow up audits where a limited assurance opinion on the control environment was reported in 2020/21 (e.g. Private Sector Empty Homes follow up review); and
- Taking into consideration other assurance providers.

The detail supporting this overview is attached at Attachment 1 which shows:

- Audit activity per service area;
- Name of the audit activity;
- Reason for the audit i.e. as a result of RBIAP, statutory requirements and/or link to Cross Cutting Risks from the Council's Excelsis (the Council's performance and risk management system) based risk register where relevant, etc;
- Outline scope of the review (please note that a detailed terms of reference is agreed with the client prior to the commencement of every audit to ensure audit activity is continually focused on the key risks and is undertaken within agreed time periods, to ensure our service adds value to the Council); and
- The priority of the audit i.e. priorities 1 and 2.

  Priority 1 reflects statutory requirements i.e. grant certification, a limited assurance follow up review, activities that may have been subject to a previous investigation / irregularity, or as deemed necessary by the Head of ARA to enable an opinion on the control environment to be provided.

  Priority 2 activities are the remaining identified activities. The aim being that all priority 1 activities would be delivered within the year with the priority 2 audits being reassessed in the eventuality of any new emerging risk areas highlighted where assurances may be required, or where additional fraud investigations/irregularities materialise.

Council Wide

Audit	Reason for Audit	Outline Scope	Priority
Business Continuity Lessons Learned	Identified as part of Risk Based Internal Audit Planning (RBIAP) Cross Cutting Risk (CCR) CCR4, 16 and 19	The Civil Contingencies Act 2004 requires all local authorities to have Business Continuity Management (BCM) arrangements in place, designed to ensure that as far as possible the local authority can continue to operate the critical elements of the service in the event of disruption such as power loss, flooded premises, high staff absence as well as other significant threats such as a pandemic. In the last 20 years there have been six significant threats: SARS, MERS, Ebola, avian influenza, swine flu and Coronavirus (Covid-19). Pandemics such as Covid-19 have the potential to severely affect the delivery of Council services. It is therefore vital that any lessons learned are captured and corrective actions taken to improve performance of the recovery process or the business continuity program. This audit will evaluate the adequacy and effectiveness of the Council's arrangements for identifying lessons learned/corrective actions, and the monitoring of implementation of these to ensure the Council's future BCM arrangements continue to improve over time.	**Priority 1**

Communities

Audit	Reason for Audit	Outline Scope	Priority
Anti-social Behaviour Management	Identified as part of RBIAP Requested by Head of Housing Services CCR4	Registered providers of social housing are required under the regulatory standards to work in partnership with other agencies to prevent and tackle anti-social behaviour in the neighbourhoods where they own homes. It is important that prompt, appropriate and decisive action is taken to deal with anti-social behaviour before it escalates, which focuses on resolving the problem having regard to the full range of tools and legal powers available. This review will seek to determine whether the current arrangements for handling reported anti-social behaviour issues are robust, operating effectively and in line with regulatory standards.	**Priority 1**

Audit	Reason for Audit	Outline Scope	Priority
Electrical Works Limited Assurance Follow Up	Identified as part of RBIAP Limited Assurance Follow Up CCR4	The Council had a contract in place for the electrical rewire and remedial works for the Council's residential properties. The contract was let in 2016 and concluded in March 2021, with the service being brought back in-house into the Council. A review of the contract management and monitoring arrangements was undertaken during 2020/21. The findings emanating from the review resulted in a Limited assurance opinion being provided in respect of the risk identification maturity and the internal control environment. This follow up audit will seek to provide assurance that the agreed actions to address the recommendations concerning the day to day electrical works operations (i.e. those still relevant to 2021/22 service delivery) have been fully implemented.	**Priority 1**
Housing Advice	Identified as part of RBIAP Requested by Strategic Director of Communities CCR4	The Housing Advice team can give advice on a wide range of housing matters including: Renting a home from a private landlord or social landlord; illegal eviction and/or harassment; rent and mortgage arrears; homelessness prevention; domestic abuse; and advice for landlords. Internal Audit will review the effectiveness of the systems and processes in place within the Housing Advice team.	**Priority 1**

Audit	Reason for Audit	Outline Scope	Priority
Housing Revenue Account (HRA) Delivery Plan	Identified as part of RBIAP Requested by Head of Housing Services CCR4	The Council's Housing Service delivers a variety of services to tenants and plays a key role in supporting the strategic aims of the Council, including: housing, economic development and health and well being. The Council has developed a business plan which sets out the Council's considered direction, service priorities, financial model and approach to the management of business risks and opportunities which includes an action plan. This review will seek to determine whether the agreed actions are being actively progressed in line with the stated target delivery dates.	**Priority 1**
Out of Hours Emergencies	Identified as part of RBIAP Requested by SLT and Audit and Standards Committee CCR10	The Council has a wealth of expertise which is used daily to deliver the 'normal' range of services expected by the public. Emergencies can happen anywhere and at any time. Therefore in the case of genuine out of office hours emergency, the Council has put in place a dedicated telephone number to handle emergency calls. The audit will review the operating effectiveness of the out of hours emergency arrangements channelled through the Council's out of hours emergency telephone number.	**Priority 1**

Audit	Reason for Audit	Outline Scope	Priority
Safeguarding	Identified as part of RBIAP CCR4	Safeguarding means protecting people's health, wellbeing and human rights and enabling them to live free from harm, abuse or neglect. The Council has a statutory responsibility and a duty of care to co-operate and report issues relating to safeguarding to the appropriate authorities and partner agencies. The audit will review the effectiveness of the Council's arrangements for ensuring it meets its statutory responsibility and duty of care to co-operate, communicate and report issues relating to safeguarding to the appropriate internal person(s), authorities and partner agencies.	**Priority 1**
Tenant Engagement	Identified as part of RBIAP Requested by Strategic Director of Communities CCR10	The Tenant Involvement and Empowerment Standard sets expectations for registered providers of social housing to provide choices, information and communication that is appropriate to the diverse needs of their tenants, a clear approach to complaints and a wide range of opportunities for them to have influence and be involved. Internal Audit will review the effectiveness of the Council's arrangements for compliance with the Tenant Involvement and Empowerment Standard.	**Priority 1**

Audit	Reason for Audit	Outline Scope	Priority
Cleaner Estates Strategy (Refuse)	Identified as part of RBIAP Requested by Strategic Director of Communities and Head of Housing Services CCR1	Tenant Services Cleaner Estate Strategy (Refuse) aims to ensure that waste, recycling and new emerging services in this area operate effectively and efficiently in order to minimise household refuse being sent for treatment and disposal. The Strategy sets out a series of actions to be delivered over the next five years with the aim of achieving better refuse management. This review will seek to determine whether the agreed actions are being actively progressed in line with the stated target delivery dates.	**Priority 2**
Voids Management	Identified as part of RBIAP Requested by Strategic Director of Communities CCR4	The Council has circa 5,000 domestic properties. Voids management is the term used to define how the Council deals with vacant property to ensure that rent loss is minimised and the most effective use is made of the Council's housing stock in order to meet housing need. This review will seek to determine whether there are effective arrangements in place to ensure good management of the Council's void properties, to limit void periods in order to maximise rental income and provide a quality service to meet housing need.	**Priority 2**

Place

Audit	Reason for Audit	Outline Scope	Priority
Canal Project Budget Management	Identified as part of RBIAP Requested by Canal Project Manager CCR1	Cotswold Canals Connected is co-led by Stroud District Council and the Cotswold Canals Trust with key partners Gloucestershire County Council, the Canal and River Trust and the Stroud Valleys Canal Company. Other partners include Gloucestershire Wildlife Trust, the Inland Waterways Association and the Stroudwater Navigation Archive charity. Stroud District Council has committed circa £3million to the project so far, with further contributions from Gloucestershire County Council, Cotswold Canals Trust and the Canal and River Trust. The total cash cost of the project, allowing for inflation and other contingencies (but excluding the value of volunteering), is £16.3million. This review will seek to determine the operating effectiveness of the project's budget management arrangements.	**Priority 1**

Audit	Reason for Audit	Outline Scope	Priority
Private Sector Empty Homes Limited Assurance Follow Up	Identified as part of RBIAP Limited Assurance Follow Up CCR1	The Stroud District Council Private Sector Housing Renewal Team works towards warm, safe, healthy homes for all the district's homeowners and private tenants. The team covers all housing which is not owned by the Council, including leasehold properties, privately rented accommodation, housing association properties and those which are owner occupied. The findings emanating from an Internal Audit review of this function as reported in July 2020 resulted in a Limited assurance opinion being provided in respect of the internal control environment. This follow up audit will seek to provide assurance that the agreed actions to address the original audit recommendations have been fully implemented.	**Priority 1**

Resources

Audit	Reason for Audit	Outline Scope	Priority
Carbon Neutral 2030	Identified as part of RBIAP Requested by Audit and Standards Committee CCR4	A Climate Emergency was announced by the Stroud District Council Administration on 16th November 2018 which pledged to "do everything within the Council's power to make Stroud District Carbon Neutral by 2030". Since the climate emergency declaration, work has been ongoing and a Strategy and supporting plan has been drafted and is pending adoption by full Council. This review will seek to determine whether the agreed actions are being actively progressed in line with the stated target delivery dates.	**Priority 1**
Creditors Limited Assurance Follow Up	Identified as part of RBIAP Limited Assurance Follow Up CCR1 and CCR4	The objective of the accounts payable function is to pay valid supplier invoices in respect of goods or services received within agreed payment terms. In 2019/20 circa £35m payments (inclusive of VAT) were processed. It is therefore important to have robust and effective controls. The findings emanating from an Internal Audit review of this function in 2019/20 resulted in a split assurance opinion being provided in respect of both the risk identification maturity and internal control environment, with a number of recommendations being made to strengthen and improve the control framework. This follow up audit will seek to provide assurance that the agreed actions to address the original audit recommendations have been fully implemented.	**Priority 1**

Audit	Reason for Audit	Outline Scope	Priority
Grant Payments Post Payment Assurance	Identified as part of RBIAP Head of Revenue and Benefits CCR1	The government has announced a range of support packages in response to the ongoing economic impact of Covid-19. Internal Audit has provided support to the Council to date to assist in ensuring that payments made are to eligible applicants. This support will continue to be provided during the financial year 2021/22.	**Priority 1**
Green Homes Grant Local Authority Delivery Scheme	Identified as part of RBIAP Strategic Director of Resources Grant CCR1	In July 2020, the Chancellor announced £2 billion of support through the Green Homes Grant (GHG) to save households money, cut carbon and create green jobs. The GHG will be comprised of up to £1.5 billion of support through energy efficiency vouchers and up to £500m of support allocated to English Local Authority delivery partners, through the Local Authority Delivery (LAD) scheme. The Council was successful in securing £1,094,050 of this grant funding. Internal Audit will undertake a series of checks in order to provide an independent opinion as to whether the scheme has been administered in line with the grant conditions, to support the grant declaration requirements of the Chief Executive and the Head of ARA.	**Priority 1**

Audit	Reason for Audit	Outline Scope	Priority
ICT	Identified as part of RBIAP (ICT Audit Needs Assessment) CCR4 and CCR16	One of the Council's corporate priorities is to invest in key ICT infrastructure that delivers better customer services, mobile working for staff and service efficiencies. The ICT Audit Needs Assessment 2021/22 has been compiled by ARA's ICT audit specialists in consultation with and having input from Council senior management (including ICT and other service areas). The 2021/22 Audit Needs Assessment identified five activities for review in year: • IT procurement process; • Incident management processes; • Change management processes (including business as usual and project); • Compliance with government standards, and • Business continuity/disaster recovery limited assurance follow up. The deferred 2020/21 consultancy review of the Council's IT Infrastructure Strategy will also be delivered within 2021/22.	**Priority 1**

Audit	Reason for Audit	Outline Scope	Priority
Lost Sales, Fees and Charges	Identified as part of RBIAP Requested by Strategic Director of Resources Grant CCR1	Covid-19 has impacted local authorities' ability to generate revenues in several service areas as a result of the pandemic. The Ministry of Housing, Communities, and Local Government (MHCLG) has introduced a one-off income loss scheme to help compensate for a proportion of the irrecoverable and unavoidable losses from sales, fees and charges income generated in the delivery of services in the financial year 2020/21. There are a total of three claims. Claim one and two have been reviewed by Internal Audit during 2020/21. Review of the third claim is required during 2021/22. The scheme also requires a reconciliation for the year (i.e. across the three claims) to ensure the account for losses claimed remain accurate and/or are adjusted accordingly. This audit will review the Lost Sales, Fees and Charges claim three (including the 2020/21 reconciliation) to provide assurance that the claim has been submitted in line with the guidance from the Ministry of Housing, Communities & Local Government (MHCLG).	**Priority 1**

Audit	Reason for Audit	Outline Scope	Priority
Procurement and Contract Management Follow Up	Identified as part of RBIAP CCR1 and CCR4	Procurement and contract management is a holistic process that combines a mix of strategic and operational tasks depending on the type of contract and the goods or services being supplied. A review of procurement and a housing contract by Internal Audit during 2020/21 highlighted two key areas for improvement: • Development / implementation of a contract management framework to support a consistent approach to contract management across the Council; and • Establishment of the function and role of the second line of defence (corporate oversight and challenge responsibilities) in order to achieve the principles and application of an effective and robust three lines of defence model. This follow up audit will seek to provide assurance that the agreed actions to address the relevant recommendations emanating from the 2020/21 audit reviews have been fully implemented.	**Priority 1**

Audit	Reason for Audit	Outline Scope	Priority
Risk Management	Identified as part of RBIAP All CCRs	The management of risk is a key process which underpins successful achievement of the Council's objectives and priorities. It is therefore paramount that the Council has clear and effective structures, strategy, and processes in place and that risk management is fully embedded and operating effectively within the Council. Internal Audit will review the effectiveness of the Council's Risk Management arrangements.	**Priority 1**
Social Housing Decarbonisation Fund Demonstrator	Identified as part of RBIAP Requested by Strategic Director of Resources CCR1	The Social Housing Decarbonisation Fund Demonstrator will start the decarbonisation of social housing over 2020 to 2021 and support green jobs as part of the government's Covid-19 recovery plan. This £50 million programme announced in July 2020 will support social landlords to demonstrate innovative approaches to retrofitting social housing at scale. It will mean warmer and more energy efficient homes, a reduction in household energy bills, and lower carbon emissions. The Council has successfully secured £991,434 of grant funding. The audit will review the effectiveness of the Council's arrangements for ensuring compliance with the terms and conditions of the grant funding.	**Priority 1**

Audit	Reason for Audit	Outline Scope	Priority
Test and Trace Support Scheme	Identified as part of RBIAP Requested by Strategic Director of Resources Grant CCR1	The Government has announced a scheme for people who are working, on a low income and who will lose money if they self-isolate. Where the grant condition criteria are met, workers will be entitled to a Test and Trace Support Payment of £500. The scheme will last until 31st March 2021. Internal Audit will undertake a series of checks in order to provide an independent opinion as to whether the scheme has been administered in line with the grant conditions, to support the grant declaration requirements of the Chief Executive and the Head of ARA.	**Priority 1**
Council Tax	Identified as part of RBIAP CCR1	Stroud District Council collects Council Tax on behalf of local authorities that issue a precept e.g. Gloucestershire County Council and Gloucestershire Police and Crime Commissioner. Council Tax requirements for 2020/21 were circa £86m within the District, with Stroud District Council's share being circa £10m. This review will seek to provide assurance that Council Tax charges have been correctly calculated, appropriately authorised, and accurately transferred to the billing system.	**Priority 2**

Audit	Reason for Audit	Outline Scope	Priority
Facilities Management	Identified as part of RBIAP Consultancy CCR1 and CCR4	Facility management is an organisational function that aids the smooth and efficient running of the Council. It integrates people, place and process within the built environment with the purpose of improving the quality of life of people, and the productivity of the Council's core business. Internal Audit will review the operating effectiveness of the Council's current arrangements with a view to help inform new service arrangements.	**Priority 2**
Purchase Cards	Identified as part of RBIAP CCR1	A purchasing card is a form of a charge card that allows goods and services to be procured without using a traditional purchasing process. The audit will review the effectiveness of the Council's arrangements for administering Purchase Cards.	**Priority 2**

Transformation and Change

Audit	Reason for Audit	Outline Scope	Priority
Fit for the Future	Identified as part of RBIAP Requested by Strategic Director of Transformation and Change Consultancy CCR4, CCR10 and CCR16	The Council committed to participating in a peer review during the latter part of 2018/19. The peer challenge offers an opportunity to validate the direction of travel and approach being taken by the Council, and test, stretch and further evolve thinking for the future. The peer review identified a number of key areas that could aid the Council's continual improvement programme. Internal Audit will provide professional advice on the future internal control environment with a view to designing out risk as the modernisation programme 'Fit for the Future' progresses.	**Priority 2**

Counter Fraud

Audit	Reason for Audit	Outline Scope	Priority
Fraud Investigation / Detection	To support the Annual Governance Statement (AGS) Protect the Public Purse	Allocation to continue the development and implementation of the Council's Anti-Fraud and Corruption arrangements based on latest best practice. This includes an allocation for increasing the profile and awareness of anti–fraud, conducting pro-active counter-fraud reviews and undertaking investigations as required. Within 2021/22, this will include focussed activity on Covid-19 relevant fraud risk themes.	**Priority 1**
National Fraud Initiative (NFI)	Statutory Requirement To support the AGS	To continue to co-ordinate activity as part of the Cabinet Office's National Fraud Initiative (NFI - a national data matching exercise that compares data/records i.e. payroll, licences, housing waiting list, single person discounts, creditors etc.) for a wide range of public services, including ensuring that matches are investigated promptly and thoroughly and reporting of results.	**Priority 1**
Fraud Risk Management	To support the AGS Informs the Risk Based Internal Audit Plan	The CIPFA Counter Fraud Centre has issued guidance on actions to be taken to 'Manage the Risk of Fraud and Corruption' within an organisation. This allocation is to continue to self assess against the criteria set out in the guidance and develop a fraud risk register in order to direct/prioritise our counter fraud and internal audit resources/activity accordingly.	**Priority 1**

Management Activity to Support the Audit Opinion

Audit	Reason for Audit	Outline Scope	Priority
Audit and Standards Committee / Member / Officer and Chief Financial Officer Reporting	Public Sector Internal Audit Standards (PSIAS) Statutory Requirement	This allocation covers Member reporting procedures, mainly to the Audit and Standards Committee, plan formulation and monitoring and regular reporting to and meeting with, the Chair and Vice Chair of the Audit and Standards Committee and the Chief Financial Officer.	**Priority 1**
Provision of Internal Control / General Advice	To support an effective control environment	This allocation allows auditors to facilitate the provision of risk and control advice which is regularly requested by officers within the Council.	**Priority 1**
Quality Assurance and Improvement Programme (QAIP)	PSIAS Statutory Requirement To support the AGS	The Accounts and Audit Regulations 2015 states that Internal Audit should conform to 'proper practices' and it is advised that proper practice for internal audit is currently set out in the Public Sector Internal Audit Standards (PSIAS) 2017. This allocation is to undertake an annual self assessment and when required, commission and deliver an external quality assessment, against the new standards.	**Priority 1**
External Working Groups	Activity to support the audit opinion	Attendance / work in relation to the Local Authorities Chief Auditor Network (National Group), Midland Counties and Districts Chief Internal Auditors Group and the Fraud and ICT Groups to enable networking and to share good practice.	**Priority 1**

Audit	Reason for Audit	Outline Scope	Priority
External Audit Liaison	Management activity to support the audit opinion	The External Auditor and the Head of ARA regularly meet to discuss plans and audit findings, to ensure that a "managed audit" approach is followed in relation to the provision of internal and external audit services.	**Priority 1**
Carry Forwards	Audit Activity outstanding	This allocation provides for the completion of various 2020/21 audits which require finalising.	**Priority 1**
Recommendation Monitoring	Activity to support the audit opinion	Whilst it is management's responsibility to manage the risks associated with their outcomes/objectives, this allocation enables Internal Audit to monitor management's progress with the implementation of high priority recommendations.	**Priority 1**
Internal Working Groups	Activity to support the audit opinion	Internal Audit is frequently asked to nominate representatives for working groups to advise on risk and control.	**Priority 2**

This page is intentionally left blank

Report to the Audit and Standards Committee 27th April 2021 on the actions taken in relation to key recommendations made in the Creditors Internal Audit report

Lead and presenting officers: Andrew Cummings, Strategic Director of Resources and Simon Killen, Revenue and Benefits Manager

Summary of Audit Area

Stroud District Council (the Council) Creditors (accounts payable) function is maintained by the Revenue and Benefits Service area. However, the Section 151 Officer has overall responsibility for ensuring the proper administration of the financial affairs of the Council.

The Workforce Plan review of Finance, which was performed by Business Service Planning, resulted in the Creditors team and function being moved to Revenue and Benefits during the second half of 2018-19.

The objective of the accounts payable function is to pay valid supplier invoices in respect of goods or services received within agreed payment terms. In 2018-19 Creditors were responsible for circa £24.9m payments (inclusive of VAT). It is therefore important to have robust and effective controls.

Summary Terms of Reference of the Audit

The review sought to determine the effectiveness of the arrangement for setting up new suppliers, supplier changes and invoice control.

The specific objectives of the audit were to provide assurance on the following areas:

- Accounts payable policy and procedures have been documented, are up to date and available to all appropriate officers;
- New suppliers are correctly set-up, authorised and subject to appropriate verification;
- Amendments to existing supplier standing data details are supported by appropriate supplier change notification, subject to effective verification and timely correct update;
- Purchase orders are raised in respect of all goods and services to ensure effective budgetary management and control;
- There is adequate separation of duties to ensure payments are only for goods and services received, including creating the requisition and purchase order, receiving the invoice and making payment;
- Commitments and invoice management is effective and robust;
- Invoices are promptly paid in accordance with Government Prompt Payment Policy and performance is reported;
- Payment runs are correctly authorised and subject to appropriate verification; and
- Creditor control and suspense account reconciliations are subject to regular reconciliation, independent review and authorisation.

Risks

- Officers are not fully aware of the agreed processes or their responsibilities resulting in financial losses and / or reputational damage due to incorrect invoice processing and / or late payments;
- Unauthorised or incorrect supplier details are set-up on the finance system for fraudulent purposes or in error resulting in financial losses and adverse publicity from fraud, payment to incorrect supplier or late payment;
- Ineffective budgetary management resulting in financial losses, reduction in the Council's commitments and / or reserves and reputational damage;
- Incorrect or fraudulent transactions are processed resulting in financial losses and adverse publicity;
- Valid and undisputed vendor invoices are not paid within the agreed payment terms resulting in adverse publicity and reputational damage;
- Duplicate payments are made resulting in financial losses and adverse publicity; and
- The Council's financial records do not correctly reflect the Authority's financial position resulting in financial losses, adverse publicity and poor management decisions.

Key Findings

Policy and Procedures

- At the point of transfer, and to date, the relationship, roles and responsibilities and communications between Finance and Revenue and Benefits concerning the accounts payable operating control environment have not been clarified / or aligned.

See recommendation one

- The Creditors team procedures manual requires a review and refresh to ensure that it is up to date and going forward that it is subject to periodic review or maintained on an ongoing basis.

See recommendation two

- Accounts payable forms are available to service areas on the Council's intranet to support process completion. However there is no procedures manual / guidance for the accounts payable process, which would aid service areas and payment authorisers to fully understand their roles and responsibilities.

See recommendation two

- Only one operational risk relating to the accounts payable process has been identified and reported on the Council's risk and performance management system Excelsis. This reported risk has not correctly identified the Control Lead Officers.

See recommendation three

New Suppliers

- A review by Internal Audit of a sample of 25 new suppliers highlighted non-compliance or weaknesses in the agreed processes as follows:
  - Supplier supporting documentation not retained by the service (four cases);
  - Lack of documentary evidence to confirm supplier details were reviewed and approved by a different service area officer (all cases); and
  - Service area submitted incomplete or incorrect supplier address or contact details to the Creditors team.

See recommendation four

Change of supplier payment and contact details

- A review by Internal Audit of a sample of 15 changes to supplier payment and contact details highlighted that:
  - There was a lack of documentary evidence to confirm the supplier payment detail changes had been checked and verified by a different Creditors officer (three suppliers); and
  - Errors or omissions with the supplier's address or contact details, updated to their record on the Business World financial system (three suppliers).

See recommendations five and six

Purchase orders

- Purchase orders are not being used in all cases, with the exception of approved case / categories, by service areas in accordance with Financial Regulations. For the current financial year to September 2019 and for the last two years the percentage of purchase orders raised against the total number of invoices received has been less than 30%.

  Finance and the Revenue and Benefits Manager have advised Internal Audit that there are currently ongoing discussions with the service areas to encourage more significant use of purchase orders.

See recommendation seven

Separation of duties

- Some service area invoice authorisers have been assigned Business World systems access to also process invoices to enable sufficient resource coverage in this area. This weakens the control environment as it enables these invoice authorisers to also process and approve the same invoice. Internal Audit is able to confirm based on the findings of sample testing of 15 invoices that no instances of the same officer processing and approving an invoice were identified.

See recommendation eight

- Five Finance officers have been assigned the Business World 'super user' systems access, which enables virtually unlimited privileges to the system. As at the point of this audit the controls over the 'super user' function is limited to 'long stop' controls such as service area budget monitoring, system audit logs (not currently reviewed), supplier notification of non-payment, etc to identify any potential unauthorised activity.

See recommendation nine

Commitments and invoice management

- There are a six key exception reports available / generated from Business World to aid officers in the identification of issues within the accounts payable process. A review by Internal Audit of these exception reports highlighted the following:
  - One weekly report to identify invoices that had been entered into Business World that had not been processed or authorised for payment after 28 days had stopped in July 2019 due to a systems issue. At the point of this audit the report was last reviewed on 21st August 2018 by the Creditors team. The report recommenced in November 2019 following Internal Audit intervention;
  - There was a lack of documentary evidence to confirm that three out of the four different types of duplicate invoice / payment exception reports had been subject to appropriate timely checks; and
  - Creditors do not receive a copy of the outstanding purchase order report that is sent to appropriate service officers and therefore are unable to ensure appropriate actions have been undertaken.

See recommendations ten and eleven

Payments performance

- The Council has not published its supplier payment terms but has set itself a performance measure to pay 97% of all invoices within 30 days of receipt of the supplier invoice or within the agreed supplier payment terms.

  The Council supplier payment performance has been reported on Excelsis for 2015-16 to June 2018, after this date no statistics have been recorded. A report obtained by Internal Audit from the System Accountant from Business World for the financial year 2018-19 shows that the Council has paid 93.46% of invoices (9,353) within 30 days following receipt of the supplier invoice; 655 invoices were paid after this period.

See recommendation twelve

- The Council has not annually published its payment performance on the Council website in accordance with the Crown Commercial Service Procurement Policy Note (PPN – Action Note 03/16).

See recommendation thirteen

Payments process

- A walkthrough by Internal Audit of the payments process and the results of fieldwork tests confirmed that the checks performed by payment authorisers were adequate and operating effectively.

Creditor control and suspense reconciliations

- Monthly creditor control and suspense reconciliations are undertaken by a Finance officer, which are subject to a detailed and evidenced check at the financial year-end by the Systems Accountant. A review of the June and September 2019 reconciliations by Internal Audit confirmed that the creditor control reconciliations had been promptly and correctly performed. However, the suspense reconciliation for September 2019 highlighted 13 outstanding transactions totalling approximately £55,000 gross with the oldest dated 26th March 2018 that had not been cleared and posted to the correct general ledger accounts.

See recommendation fourteen

Conclusion

Suppliers are being promptly paid, albeit not all within the Council's or Crown Commercial Services performance target. In addition there has been no reported unauthorised activity during the audit period.

Internal Audit's review and sample testing of the accounts payable processes has found that the majority of recognised processes and controls that would be expected by Internal Audit are in place. However, these were found to not always being fully applied or operating effectively and improvements / enhancements are required to strengthen the overall control framework. As a result Internal Audit has provided a split opinion for the control environment as follows:

- Satisfactory assurance – suitable controls for the accounts payable process have been introduced; and
- Limited assurance – controls have not been fully applied or are operating effectively.

As noted above management have introduced a range of controls in the accounts payable process that indicates that they have considered the risks to the Council and established their risk appetite. However, these operational risks and risk appetite have not been formally documented on Excelsis and also there is a lack of evidence to confirm they are being regularly managed. Therefore Internal Audit has also provided a split opinion on risk maturity as follows;

- Satisfactory assurance – adequate awareness of the risks relating to the accounts payable process; and
- Limited assurance – absence of accurate and regular risk reporting and monitoring.

Two high and twelve medium priority recommendations have been raised to strengthen and improve the control framework and to ensure existing controls operate effectively.

The Strategic Director of Resources and Revenue and Benefits Manager have confirmed that they will work together to revise the accounts payable working procedures to ensure they are effective and adequately manage the known inherent risks in the process.

Action(s) taken to implement the recommendations as at February 2021 and / or proposed.

High priority recommendation 1: Finance and Creditors team roles and responsibilities for the accounts payable processes	**Original management response**
The Strategic Director of Resources and the Revenue and Benefits Manager should determine Finance and Creditors team roles and responsibilities for the accounts payable processes that ensure clear ownership, accountability and effective management and control. The results of this review should be documented and Finance officer Business World systems access updated accordingly.	Finance and Creditors staff are to work together to revise creditors working procedures. This will focus on effective processes and management of risk. Clearly the response to Covid-19 has delayed this to some extent but it will be completed in 2020/21. To a greater or lesser extent this action applies to all recommendations within this report. **Completion date:** 31st December 2020
Management update as at February 2021:	
This piece of work is underway although not yet complete. There has been a continued impact of Covid-19 financial support schemes on the work pressure of the team.	

Medium priority recommendation 2: Formalisation of Accounts Payable process procedure manual / guidance	**Original management response**
A comprehensive Accounts Payable process procedure manual / guidance to be formalised. This should include the agreed roles and responsibilities as defined as an outcome of recommendation 1. Staff to be made aware of, and have ongoing access to the new procedures / guidance and if deemed appropriate, staff training to be given.	As per recommendation 1 procedures are to be refreshed and documentation updated. **Original Completion date:** 31st December 2020 **Revised Completion Date:** 30th September 2021
Management update as at February 2021:	
This has not yet been started as the team has been focusing on the additional work relating to Business Grants/ Track & Trace payments. During this time a member of staff has also left the team, further increasing the pressure on workload.	

High priority recommendation 3: Identification of operational risks and associated mitigating controls, risk owners, etc.	**Original management response**
A review of the accounts payable processes should be undertaken to identify all operational risks and associated mitigating controls, risk owners etc. These should be recorded within Excelsis, and where appropriate amendments made to the mitigating control owners currently reported against the one documented accounts payable risk. This will ensure visibility of the inherent and residual risks, and their ongoing management and monitoring.	See Recommendation 1 and 2. **Original Completion date:** 31st December 2020 **Revised Completion Date:** 30th September 2021

Management update as at February 2021:
The risk assessment has been discussed with the Systems Accountant and a risk score of 4 assessed - New Excelsis risk assessments to be set up with assistance from Policy & Performance officer and will be in place by 31st March 2021.

Medium priority recommendation 4: Re-evaluate current position and risk appetite for the request and setting up of new suppliers	**Original management response**
Revenue and Benefits management with support from Finance should re-evaluate the current position and risk appetite for the request and setting up of new suppliers based on Internal Audit observations and should either: • Strengthen the control environment by ensuring that only appropriately approved service area new supplier set-up requests are accepted by the Creditors team with all supporting documents for new suppliers provided to the Creditors team to verify and retain on the supplier Business World record, which Internal Audit supports; or • Accept the risks and document this risk appetite in Excelsis.	As part of the review of the procedures this will include the risk position. **Original Completion date:** 31st December 2020 **Revised Completion Date:** 30th April 2021
Management update as at February 2021:	
The risk assessment has been discussed with the Systems Accountant and a risk score of 4 assessed - New Excelsis risk assessments to be set up with assistance from Policy & Performance officer.	

Medium priority recommendation 5: Changes to Business World system	Original management response
Changes to the Business World system should be explored with the systems software supplier to enable system enforcement of two different officers (input and verification / approval) for amendments to supplier payment, address and contact details. If the system cannot be configured appropriately then regular independent checks should be undertaken to confirm the existing controls are operating effectively.	This will be explored as part of the review of service procedures. **Original Completion date:** 31st December 2020 **Revised Completion Date:** 30th September 2021
Management update as at February 2021:	
A Unit 4 upgrade in January 2021 gives functionality for supplier updates to be completed within the system, with an authorisation process in place. This work will be scoped out and will require additional resource (officer and consultant time) in order to implement.	

Medium priority recommendation 6: Supplier contact	Original management response
Suppliers should be contacted in all cases when there is a request or notification of a change of payment, address or contact details to confirm the amendments are genuine. In addition a pro forma should be created to record the checks required to be completed with the supplier, evidence of the checks and secondary confirmation checks by a different person.	This will be explored as part of the review of service procedures. **Completion date:** 31st December 2020

Management update as at February 2021:
Suppliers are contacted when changes are required and copies of confirmation of changes are scanned to Unit 4. Bank changes are checked by 2 officers. These changes will be included when looking at potential changes to Unit 4 as included in Recommendation 5. There will also be consideration of system enhancements to highlight supplier changes & new suppliers for additional checks prior to each payment run.

Medium priority recommendation 7: Full usage of purchase orders	**Original management response**
Finance and Revenue and Benefits management should actively pursue full usage of purchase orders by service areas in compliance with the Financial Regulations and to support accurate budgetary management and a good control environment.	Purchase Order (PO) use has grown significantly in the previous 12 months. Plans were in place to enforce return of invoices without a PO number but this was relaxed during the Covid response. Moving forward in 2020/21 this will be enforced and monitored. **Original Completion date:** 31st December 2020 **Revised Completion Date:** 30th September 2021
Management update as at February 2021:	
Ongoing – relevant Service Units have been given guidance on how to raise Purchase Orders & are actively raising PO's. Invoices are being returned to users for PO's prior to invoice being input to Unit 4. The next stage is writing to all suppliers to advise them of a "No Po No Payment Policy". This requires a large amount of data that has to be pulled from the system and has been temporarily delayed by Covid-19 work pressures within the team. Despite the challenges of the last year the use of purchase orders has increased from 31% of invoices paid in February 2020 to 60% in February 2021. Further work will be undertaken with services and suppliers to increase this further.	

Medium priority recommendation 8: Segregation of duties	Original management response
Invoice authorisers Business World systems access to process an invoice (without a purchase order) should be removed to ensure segregation of duties between invoice processing and authorisation.	Segregation of Duties is often a challenge for District Councils where team sizes do not always allow for such clear distinctions. The control test here clearly shows the control functioning but the review of processes will consider how this functions in future. **Completion date:** 31st December 2020
Management update as at February 2021:	
Coding access from authorisers has been removed in line with the recommendation.	

Medium priority recommendation 9: Review of user Business World systems access	Original management response
The following review of user Business World access should be undertaken: • Re-assess whether the number of officers with the 'super user' access be further restricted and to introduce additional controls such as independent monitoring over its usage; • Review all users who have been assigned two user access profiles on the Business World system to ensure that it is required and does not erode the segregation of duties control; and • Review the use and operation of generic user identifications, due to their lack of accountability, to establish whether their continued use is necessary / required.	It will always be necessary to have a number of officers with super-user access to ensure reliance in providing the service. However, a review will be carried out of both super users and generic user identifications. **Completion date:** 31st December 2020
Management update as at February 2021:	
All user accounts are reviewed monthly by the Systems Accountant.	

Medium priority recommendation 10: Independent monitoring checks of exception reports	Original management response
Regular (at least quarterly) independent monitoring checks should be undertaken to confirm exception reports have been promptly and correctly actioned. The Creditors team should receive a copy of the monthly report of outstanding purchase orders to chase up long outstanding purchase orders with service area management.	Outstanding purchase orders will be regularly reviewed and those which have been outstanding for more than 12 months are deleted. **Completion date:** 31st December 2020
Management update as at February 2021:	
Outstanding PO's are checked by the budget team and access to the report has been provided to Creditors team.	

Medium priority recommendation 11: Record of incorrect and duplicate payments	Original management response
A record of all incorrect and duplicate payments should be made and used to support recovery of the debt. This report should also be subject to regular (at least quarterly) management review.	A record will be kept of any duplicate payments identified. **Completion date:** 31st December 2020
Management update as at February 2021:	
Duplicate Payment report produced regularly & checked by Creditors Team – reports filed & available for inspection.	

Medium priority recommendation 12: Payment performance reports	Original management response
Regular (at least quarterly) payment performance reports should be obtained from Business World and subject to review by the Revenue and Benefits Manager to enable effective monitoring of the performance, introduction of corrective measures if appropriate and update to Excelsis.	Payment performance to be reviewed when selected for publication (see next recommendation). **Completion date:** 31st December 2020
Management update as at February 2021:	
Report now sent to Creditors Team monthly & quarterly – Excelsis for 2020/21 now up to date.	

Medium priority recommendation 13: Publication of payment performance	Original management response
The Council should annually publish its payment performance on the Council website in accordance with the Crown Commercial Service Procurement Policy Note (PPN – Action Note 03/16).	Agreed – This will be published. **Completion date:** 31st December 2020
Management update as at February 2021:	
Although figures are now produced they are not yet published externally – With the support of the information governance officer in the Policy and Governance team figures will be published for the new financial year in line with our transparency obligations.	

Medium priority recommendation 14: Creditor control and suspense reconciliations independent checks	Original management response
Monthly detailed independent checks on the monthly creditor control and suspense reconciliations should be performed and evidenced to confirm prompt reconciliation completion and that any unmatched / outstanding transactions reported are being thoroughly investigated and cleared on a timely basis.	Reconciliation procedures are already carried out as part of year end procedures and balances will be reviewed as part of external audit. Mid-year recs will be considered but monthly is likely to be disproportionate to level of risk. **Completion date:** 31st March 2021
Management update as at February 2021:	
A year-end reconciliation is on going.	

This page is intentionally left blank

STROUD DISTRICT COUNCIL **AGENDA ITEM NO**

AUDIT AND STANDARDS COMMITTEE

27 APRIL 2021 **9**

Report Title	**3RD QUARTER TREASURY MANAGEMENT ACTIVITY REPORT 2020/21**			
Purpose of Report	To provide an update on treasury management activity as at 31/12/2020.			
Decision(s)	**The Audit and Standards Committee RESOLVES to note the treasury management activity third quarter report for 2020/2021.**			
Consultation and Feedback	Link Asset Services (LAS).			
Report Author	Maxine Bell, Snr Accounting Officer Tel: 01453 754134 E-mail: maxine.bell@stroud.gov.uk			
Options	None			
Background Papers	None			
Appendices	Appendix A – Prudential Indicators as at 31 December 2020 Appendix 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 is 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. A quarterly report is regarded as good practice, but is not essential under the Code of Practice for Treasury Management (the Code).

Discussion

3. The Chartered Institute of Public Finance and Accountancy (CIPFA) issued the revised Code in November 2011, 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 2020/21
- A review of the Council's borrowing strategy for 2020/21
- A review of compliance with Treasury and Prudential Limits for 2020/21.
- Other Treasury Issues

Treasury Management Strategy Statement and Investment Strategy update#

4. The TMSS for 2020/21 was approved by Council on 20th February 2020. The Council's Investment Strategy, which is incorporated in the TMSS, outlines the Council's investment priorities as follows:
    1. Security of Capital
    2. Liquidity
    3. Yield

5. In 2020-21 the Council will continue to invest for the longest permitted duration with quality counterparties to maximise return without compromising security, or liquidity. In particular instances the Section 151 Officer will authorise investments in the LAS blue category for a period of up to two years, which is currently longer than the LAS recommended duration of one year. Otherwise, the length of investments permitted will vary if necessary in line with LAS advice subject to the Council's 3-year upper limit.

6. A breakdown of the Council's investment portfolio as at 31st December 2020 is shown in Table 2 and 3 of this report. Investments & borrowing during the year have been in line with the strategy.

Investment Portfolio 2020/21

7. 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 is shown in the table below:

TABLE 1: Average Interest Rate Compared With Benchmark Rates

	Period	Investment Interest Earned £	Average Investment £m	Rate of Return	Benchmark Return 7 day LIBID uncompounded	For comparison 3 month LIBID uncompounded
Internally Managed Specified	01/04/2020 - 30/06/2020	49,874	46.444	0.422%	-0.04%	0.26%
Property Fund / Multi-Asset Fund		54,649	8.763	2.47%	-0.04%	0.26%
Total Quarter 1		**104,523**	**55.207**	**0.75%**	**-0.04%**	**0.26%**
Internally Managed Specified	01/07/2020 - 30/09/2020	34,997	48.928	0.284%	-0.07%	-0.06%
Property Fund / Multi-Asset Fund		68,430	8.872	3.08%	-0.07%	-0.06%
Total Quarter 2		**103,427**	**57.800**	**0.72%**	**-0.07%**	**-0.06%**
Internally Managed Specified	01/10/2020 - 31/12/2020	27,142	52.013	0.207%	-0.08%	-0.08%
Property Fund / Multi-Asset Fund		71,367	10.001	2.787%	-0.08%	-0.08%
Total Quarter 3		**98,509**	**62.014**	**0.64%**	**-0.08%**	**-0.08%**
TOTAL	01/04/2020 - 30/12/2020	**306,459**	**58.340**	**1.58%**	**-0.07%**	**0.04%**

TABLE 2: Funds Performance – Quarter 3 2020-21

Fund	Initial Investment £m	Value as at 31/12/2020 £m	Return Apr - Dec 2020
Lothbury	4.000	3,829	2.54%
Hermes	2.000	1,927	3.80%
Royal London	3.000	3,227	2.34%
CCLA	1.000	1,018	3.83%
TOTAL	**£10,000**	**£10,001**	**2.787%**

8. The approved limits as set out in the Treasury Management Strategy report to Council 20th February 2020 within the Annual Investment Strategy were not breached during the first 9 months of 2020/21.

9. Funds were available for investment on a temporary basis. The level of funds available was mainly 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.

10. Table 3 below shows the investments and borrowing position at the end of December 2020

TABLE 3: Investments & Borrowing

	Jun 2020 £'000		Sep 2020 £'000		Dec 2020 £'000	
Aberdeen	3,323		3,994		3,962	
Federated Prime Rate	4,000		3,109		1,129	
Deutsche	0		1		8	
Goldmans Sachs	1		1		1,197	
Money Market Funds Total		**7,324**		**7,105**		**6,296**
Bank of Scotland	0		0		0	
Lloyds	7,977		7,981		7,983	
Lloyds Banking Group Total		**7,977**		**7,981**		**7,983**
NatWest	0		**1**		1580	
Royal Bank of Scotland	8		3,008		3,008	
RBS Banking Group Total		**8**		**3,009**		**4,588**
Standard Chartered	4,000		2,000		2,000	
Santander	7,959		7,969		7,978	
Barclays Bank Plc	7,753		7,758		7,999	
Svenska Handelsbanken	7,988		7,994		7,995	
DMO	0		0		500	
North Lanarkshire Council	0		0		3,000	
Thurrock District Council	0		0		2,000	
Dudley Metropolitan Council	1,000		1,000		1,000	
Other Banks Total		**28,700**		**26,721**		**32,472**
Coventry Building Society	0	**0**	6,000	**6,000**	8,000	**8,000**
SHORT TERM INVESTMENTS		**£44,009**		**£50,816**		**£59,339**
Property Funds		5,830		5,686		5,757
Diversified Funds		3,045		3,117		4,245
TOTAL INVESTMENTS		**£52,884**		**£59,619**		**£69,341**
PWLB		103,717		103,717		103,717
TOTAL BORROWING		**£103,717**		**£103,717**		**£103,717**

External Borrowing

11. The Council's Capital Financing Requirements (CFR) for 2020/21 is £115.05m. 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 £103.717m as at 31st December 2020.

Compliance with Treasury and Prudential Limits

12. 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.

13. During the period to 31st December 2020 the Council has operated within treasury limits 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.

4. IMPLICATIONS

4.1 Financial Implications

There are no financial implications arising from the decision. The whole report is of a financial monitoring nature.

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

4.2 Legal Implications

There are no specific legal implications arising from the recommendations in this report.

Patrick Arran, Interim Head of Legal Services & Monitoring Officer
Tel: 01453 754369 Email: patrick.arran@cotswold.gov.uk

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 in this report.

Prudential Indicators as at December 2020

Prudential Indicator	2020/21 Indicator £'000	Actual as at 30 June 2020 £'000	Actual as at 30 Sept 2020 £'000	Actual as at 31 Dec 2020 £'000
Capital Financing Requirement (CFR)	115,049	110,014	112,253	113,651
Gross Borrowing	105,717	103,717	103,717	103,717
Authorised Limit for external debt	137,000	103,717	103,717	103,717
Operational Boundary for external debt	129,000	103,717	103,717	103,717
Principal sums invested > 365 days	15,000	9,000	9,000	11,000
Maturity structure of borrowing limits				
Under 12 months	25%	1%	1%	1%
12 months to 2 years	50%	0%	0%	0%
2 years to 5 years	75%	2%	2%	2%
5 years to 10 years	100%	0%	0%	0%
10 years and above	100%	97%	97%	97%

This page is intentionally left blank

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 2020 strategy with actual gross borrowing as at 30 December 2020.

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 £113.651m provides the Council with the opportunity to borrow if appropriate. £7.5m of borrowing is planned for 2020/21 arising from the approved capital programme, together with £1.9m 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 2020 to 30 December 2020.

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 2020 to 30 December 2020.

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 14 of the latest Treasury Management Strategy.

This page is intentionally left blank

STROUD DISTRICT COUNCIL **AGENDA ITEM NO**

AUDIT AND STANDARDS COMMITTEE

27 APRIL 2021 **10**

Report Title	**COUNTER FRAUD UNIT REPORT AND REGULATION OF INVESTIGATORY POWERS ACT (RIPA) 2000 / INVESTIGATORY POWERS ACT (IPA) 2016 REPORT**			
Purpose of Report	To provide the Audit and Standards Committee with assurance over the counter fraud activities of the Council in relation to the work undertaken by the Counter Fraud Unit (CFU). The report is presented to the Audit and Standards Committee detailing progress and results for consideration and comment as the body charged with governance in this area. The report also provides the Audit and Standards Committee with two Policies, for approval and adoption, in relation to the Regulation of Investigatory Powers Act 2000, the Investigatory Powers Act 2016 and the Council's existing Policies and arrangements.			
Decision(s)	**The Committee RESOLVES to:** **a) Note the CFU updates;** **b) Approve and adopts the revised Regulation of Investigatory Powers Act 2000 Surveillance and Covert Human Intelligence Source Policy as attached at Appendix 1;** **c) Approve and adopt the new Investigatory Powers Act 2016 Acquisition of Communications Data Policy as attached at Appendix 2, and** **d) Authorise the Monitoring Officer to approve future minor amendments to the Policies in consultation with the Counter Fraud Unit Manager.**			
Consultation and Feedback	Work provision for 2020/2021 was agreed with the Strategic Director of Resources. The Policies were subject to consultation with the Monitoring Officer and One Legal.			
Report Author	Emma Cathcart, Counter Fraud Unit Manager Tel: 01285 623356 Email: Emma.Cathcart@cotswold.gov.uk			
Options	None. The CFU is a specialist criminal enforcement service working with the Gloucestershire Local Authorities, West Oxfordshire District Council and a number of other public sector bodies such as social housing providers.			
Background Papers	None			
Appendices	Appendix A - Regulation of Investigatory Powers Act 2000 Surveillance and Covert Human Intelligence Source Policy. Appendix B - Investigatory Powers Act 2016 Acquisition of Communications Data Policy.			
Implications (further details at the end of the report)	Financial	Legal	Equality	Environmental
	Yes	Yes	Yes	No

1. INTRODUCTION / BACKGROUND

1.1. 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.

1.2. A summary of the work undertaken during 2020/2021 is presented to the Audit and Standards Committee detailing progress and results for consideration and comment as the body charged with governance in this area. Work plans are agreed with senior management. Currently plans may be subject to change as a consequence of the work streams created by the Covid-19 Pandemic.

1.3. The Council is required to proactively tackle fraudulent activity in relation to the abuse of public funds. The Counter Fraud Unit provides assurance in this area. Failure to undertake such activity would accordingly not be compliant and expose the authority to greater risk of fraud and/or corruption. If the Council does not have effective counter fraud and corruption controls it risks both assets and reputation.

1.4. The Regulation of Investigatory Powers Act and Investigatory Powers Act Policies set out the legislative framework and principles the Council will abide by to mitigate the risk of legal challenge in Court.

1.5. The Policies demonstrate the Council's consideration of necessity, proportionality and public interest when deciding on surveillance activity and requests for communication data. It also demonstrates openness and transparency for its customers.

2. MAIN POINTS

2.1. **Counter Fraud Unit Update.**

2.2. As a dedicated investigatory support service, the CFU 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.

2.3. The CFU 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.

2.4. During 2020/2021, the team have received 3 referrals and closed 9 cases. This resulted in the following:

- 3 successful prosecutions:
    - Case 1 - 2 defendants, both pleaded guilty. The first defendant received a 24 week custodial sentence suspended for 18 months and a 6 month Curfew Order. The second defendant received a 36 week custodial sentence suspended for 18 months and 60 hours Community Service / Unpaid Work Order. The increased Council Tax revenue or fraudulently claimed Council Tax Support totalled £4,142.
    - Case 2 – defendant pleaded guilty and will be sentenced on 17 May 2021. The increased Council Tax revenue or fraudulently claimed Council Tax Support totalled £2,239. Additionally there is also an overpayment of £1,174 in discretionary housing payments to be repaid.

- The application of 5 Civil Penalties and 1 Criminal Penalty totalling £817, and increased Council Tax revenue of £2,106 being raised.
- The team have processed 3 enquiries for DWP.

2.5. 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.

2.6. The CFU are assisting the Revenues and Benefits Department with the review of National Fraud Initiative (NFI) matches. Work will commence in April on matches relating to Council Tax Single Person Discount anomalies, results will be reported accordingly.

2.7. The CFU continues to support the Council in tackling tenancy fraud. The overall remit of the CFU 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 CFU will continue to work with the Council 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. During 2020/2021, the team have received 3 new cases and closed 9 cases. There are 10 active investigations and the team are working with officers in the Housing Team to progress matters. Outcomes will be reported accordingly.

2.10. **Regulation of Investigatory Powers Act (RIPA) 2000 and Investigatory Powers Act (IPA) 2016.**

2.11. The Council's Policies are based on the legislative requirements of the Regulation of Investigatory Powers Act 2000, the Investigatory Powers Act 2016 and the Codes of Practice relating to directed surveillance, the use of covert human intelligence sources and the acquisition of communications data. Attached at Appendix 1 and at Appendix 2 are revised and newly drafted Policies. These Policies have been reviewed by the Investigatory Powers Commissioner's Office Inspector during the course of recent partner Council inspections and the suggested minor amendments have been incorporated.

2.12. The Investigatory Powers Act 2016 now governs communication data requests. Communication data can include the address to which a letter is sent, the time and duration of a communication, the telephone number or email address of the originator and recipient, and the location of the device from which the communication was made. It covers electronic communications including internet access, internet telephony, instant messaging and the use of applications. It also includes postal services. It does not include the content of any communication. It is not lawfully possible for Council employees under any circumstances to obtain the content of communications.

2.13. The legislation widened the scope of information Local Authorities may obtain for investigations, introduced the necessity for a serious crime threshold and removed the requirement for judicial approval.

2.14. All applications for communications data are made online via the National Anti-Fraud Network (NAFN) which acts as the single point of contact for Local Authorities. NAFN send requests to the Office for Communication Data Authorisations (OCDA) which ratifies all applications from public authorities for approval and if granted, NAFN will then obtain the requested data for the applicant.

2.15. There is a requirement for the Local Authority to nominate a Designated Senior Officer who will confirm to NAFN that the Local Authority is aware of any request and approve its submission. This role will be undertaken by the Information Governance Officer with assistance from the Counter Fraud Unit Manager.

2.16. Surveillance and the use of a Covert Human Intelligence Source (CHIS) is still governed by the Regulation of Investigatory Powers Act 2000 and any 'RIPA' applications are subject to the same application processes as outlined in the previous Policy – the offence must meet the serious crime threshold and the Local Authority must obtain judicial approval.

2.17. The refreshed Policy introduces a mandatory requirement for staff to complete a Non-RIPA Application Form where surveillance is being undertaken but the offence does not meet the serious crime criteria.

2.18. The Local Authority must have a Senior Responsible Officer and Authorising Officers to approve the application before the Court is approached. The Senior Responsible Officer is the Chief Executive and the Authorising Officers are the Monitoring Officer and the Head of Environmental Health.

2.19. The role of RIPA Coordinator will be undertaken by the Information Governance Officer, with assistance from the Counter Fraud Unit Manager, who will be responsible for the management of Policies, annual updates to Members, the return of statistics to the Investigatory Powers Commissioners Office, coordination of any inspections by the Investigatory Powers Commissioners Office and the management and recording of all applications by Officers of the Local Authority.

2.20. 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.

2.21. There have been no RIPA applications and no applications for communications data. The Council has not held data relating to Non-RIPA activity to date.

3. CONCLUSION

3.1 The Council were fully supportive of the original Counter Fraud Unit project and funding bid and the CFU is now delivering financial results in this area.

4. IMPLICATIONS

4.1 Financial Implications

4.1.1 The report details financial savings generated by the Counter Fraud Unit.

4.1.2 The adoption and approval of these Policies will support the Council's objectives in reducing crime and financial loss to the Local Authority.

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 Council is 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. It should also consider government guidance in this area.

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 the Policy.

4.2.4 Any requests for directed/covert surveillance or the acquisition of communications data to be undertaken should be necessary and proportionate, and authorised by the appropriate Officer. Both Policies provide information and advice to those seeking authorisation and those officers granting authorisation. Both policies confirm the process to be used and matters to be considered.

Patrick Arran, Monitoring Officer
Email: patrick.arran@stroud.gov.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.

4.3.2 The application of these Policies, to govern surveillance and the obtaining of personal communications data, ensures that there is less risk that an individual's human rights will be breached. Furthermore it protects the Council from allegations of the same.

4.4 Environmental Implications

4.4.1 There are no significant implications within this category.

This page is intentionally left blank

Regulation of Investigatory Powers Act 2000
Surveillance and Covert Human Intelligence Source Policy

Version Control:	
Document Name:	Regulation of Investigatory Powers Act 2000 Surveillance and Covert Human Intelligence Source Policy
Version:	2
Responsible Officer:	Emma Cathcart, Counter Fraud Unit
Approved by:	
Date First Approved:	TBC
Next Review Date	
Retention Period:	N/A

Revision History

Revision date	**Version**	**Description**
April 2019	2	Change in legislation / introduction of IPA 2016

Consultees

Internal	**External**
Audit Committee	
Legal Department	
Corporate Management	

Distribution

Name	
Enforcement Officers	

CONTENTS

1. INTRODUCTION

1.1 The performance of certain investigatory functions by Local Authorities may require the surveillance of individuals or the use of undercover Officers and informants. Such actions may intrude on the privacy of individuals and can result in private information being obtained and as such, should not be undertaken without full and proper consideration. The Regulation of Investigatory Powers Act 2000 (RIPA) regulates these types of activities and the Act and this Policy must be followed at all times.

1.2 Neither RIPA nor this Policy covers the use of any overt surveillance, or general observation that forms part of the normal day to day duties of Officers, or circumstances where members of the public volunteer information to the Council. The majority of the Council's enforcement functions are carried out in an overt manner.

1.3 RIPA was introduced 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. This reflects the requirements of Article 8 (right to privacy) under the HRA. RIPA provides a statutory mechanism for authorising covert surveillance and the use of a covert human intelligence source (CHIS).

1.4 RIPA also introduced a legal gateway for public authorities to apply for telecommunications and postal data. However, these have been amended by the Investigatory Powers Act 2016 (IPA), and for guidance in relation to the obtaining of Communications Data please see the IPA Acquisition of Communications Data Policy.

2. SCOPE OF POLICY

2.1 The purpose of this document is to ensure that the Council complies with RIPA.

2.2 This document provides guidance on the regulation of any Directed Covert Surveillance that is carried out by the Council. This includes the use of undercover Officers and informants, known as Covert Human Intelligence Sources (CHIS).

2.3 Covert surveillance will only be used by the Council where it judges such use to be necessary and proportionate to the seriousness of the crime or matter being investigated.

2.4 All directed surveillance must be authorised and conducted in accordance with RIPA. Therefore, all Officers involved in the process must have regard to this document and the statutory Codes of Practice issued under section 71 RIPA. The Codes of Practice are available from:

https://www.gov.uk/government/collections/ripa-codes#current-codes-of-practice

2.5 There must be no situation where a Council Officer engages in covert surveillance without obtaining authorisation in accordance with the procedures set out in this document and the RIPA Codes of Practice.

2.6 Any queries concerning the content of the document should be addressed to the RIPA Coordinator, Counter Fraud Unit.

3. BACKGROUND

3.1 RIPA provides a legal framework for the control and regulation of covert surveillance techniques which public authorities undertake as part of their duties. As was highlighted in the introduction to this Policy, the need for such control arose as a result of the HRA. Article 8 of the European Convention on Human Rights states that:-

1) Everyone has the right of respect for his private and family life, his home and his correspondence.

2) There shall be no interference by a Public Authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health and morals or for the protection of the rights and freedoms of others.

3.2 The right under Article 8 is a qualified right and public authorities can interfere with this right for the reasons given in 2.3 above. RIPA provides the legal framework for lawful interference.

3.3 However, under RIPA, Local Authorities can only authorise directed covert surveillance for the purpose of preventing or detecting conduct which constitutes a criminal offence which is:

- An offence that is capable of attracting a maximum prison sentence of 6 months or more punishable whether on summary conviction or indictment meets the serious crime threshold or,
- Relates to the underage sale of alcohol or tobacco.

3.4 Furthermore, the Council's authorisation can only be given effect once an Order approving the authorisation has been granted by a Justice of the Peace (JP).

3.5 The serious crime criteria do not apply to CHIS authorisations.

3.6 RIPA ensures that any surveillance undertaken following a correct authorisation and approval from a JP is lawful and therefore protects the Council from legal challenge. It allows the information obtained to be used as evidence in the investigation. It can also be used if required in other investigations.

4. SURVEILLANCE WITHOUT RIPA

4.1 Section 27 of RIPA provides that surveillance shall be lawful for all purposes if authorised and conducted in accordance with an authorisation granted under RIPA.

4.2 Lawful surveillance is exempted from civil liability.

4.3 Although not obtaining authorisation does not make the surveillance unlawful per se, it does have some consequences:-

- Evidence that is gathered may be inadmissible in court;
- The subjects of surveillance can bring their own proceedings or defeat proceedings brought by the Council against them on human rights grounds i.e. we have infringed their rights under Article 8;
- If a challenge under Article 8 is successful, the Council could face a claim for financial compensation;

- The Government has also introduced a system of tribunal to deal with complaints. Any person who believes that their rights have been breached can have their complaint dealt with by the Investigatory Powers Tribunal (IPTC) (See Complaints section within the Code of Practice)

5. INDEPENDENT OVERSIGHT

5.1 From 1 September 2017 oversight of RIPA is provided by the Investigatory Powers Commissioner's Office (IPCO). They are the independent inspection office whose remit includes providing comprehensive oversight of the use of the powers to which the RIPA Codes of Practice apply, and adherence to the practices and processes described in it. They also provide guidance to be followed which is separate to the codes.

5.2 Anyone, including anyone working for the Council, who has concerns about the way that investigatory powers are being used, may report their concerns to the IPCO

5.3 IPCO has unfettered access to all locations, documentation and information systems as is necessary to carry out its full functions and duties and it will periodically inspect the records and procedures of the Council to ensure the appropriate authorisations have been given, reviewed, cancelled, and recorded properly.

5.4 It is the duty of any person who uses these powers to comply with any request made by a Commissioner to disclose or provide any information required for the purpose of enabling them to carry out their functions.

5.5 It is important that the Council can show it complies with this Policy and with the provisions of RIPA.

6. LEGAL ADVICE

6.1 The Council's legal representatives will provide legal advice to staff making, renewing or cancelling authorisations. Requests and responses for legal advice will be in writing and copied to the RIPA Coordinator, Counter Fraud Unit to keep on file.

7. REVIEW OF POLICY AND PROCEDURE

7.1 The Audit Committee will receive annual reports regarding the use of RIPA. Those reports will contain information on:

- Where and when the powers have been used;
- The objective;
- The authorisation process;
- The job title of the Senior Responsible Officer (SRO), Authorising Officers (AO) and RIPA Coordinator;
- The outcomes including any legal court case;
- Any costs.

8. RIPA ROLES AND RESPONSIBILITIES

8.1 THE SENIOR RESPONSIBLE OFFICER

8.2 The SRO has responsibility for the following:

- The integrity of the process in place within the Council to authorise Directed and Intrusive Surveillance;
- Compliance with the relevant sections of RIPA and the Codes of Practice;
- Oversight of the reporting of errors to the Investigatory Powers Commissioner (IPC) and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- Engagement with the IPCO and the inspectors who support the IPC when they conduct their inspections;
- Where necessary, overseeing the implementation of any recommended post-inspection action plans and;
- Ensuring that all AO are of an appropriate standard, addressing any recommendations and concerns in the inspection reports prepared by the IPC.

8.3 THE RIPA COORDINATOR

8.4 The RIPA Coordinator is responsible for storing all the original authorisations, reviews, renewals and cancellation forms and the signed approval or refusal documentation from the JP. This will include any authorisations that have not been authorised by the AO or refused by a JP.

8.5 The RIPA Coordinator will:

- Keep the copies of the forms for a period of at least 3 years;
- Keep the Central Register (a requirement of the Codes of Practice) of all of the authorisations, renewals and cancellations; and issue a unique reference number. This record should contain the information outlined within the Covert Surveillance and Property Interference revised Code of Practice;
- Keep a database for identifying and monitoring expiry dates and renewal dates;
- Along with Officers (AO and Investigating Officers (IO)), ensure that any electronic and paper records relating to a RIPA investigation are used, retained or destroyed in line with the Council's Information Management Policies, Departmental Retention Schedules and Data Protection Legislation /Regulations;
- Provide administrative support and guidance on the processes involved;
- Not provide legal guidance or advice;
- Monitor the authorisations, renewals and cancellations with a view to ensuring consistency throughout the Council;
- Monitor each department's compliance and act on any cases of non-compliance;
- Provide training and further guidance and awareness of RIPA and the provisions of this Policy; and review the contents of this Policy.

8.6 INVESTIGATING OFFICER/APPLICANT

8.7 The applicant is normally an IO who completes the application section of the RIPA form. IOs should think about the need to undertake directed surveillance or the use of a CHIS before they seek authorisation. IOs must consider whether they can obtain the information by using techniques other than covert surveillance. Advice can be given by the RIPA Coordinator.

8.8 The applicant or IO must carry out a feasibility study and this should be seen by the AO. The IO seeking authorisation should then complete the application form having regard to the guidance given in this Policy and the statutory Codes of Practice. There should not be any significant delay between the feasibility study and the completion of the application form in order to ensure that the details within the application are accurate. The form should then be submitted to the AO for authorisation.

8.9 AUTHORISING OFFICERS

8.10 The role of the AO is to authorise, review, renew and cancel directed surveillance.

8.11 AOs should not be responsible for authorising investigations or operations in which they are directly involved. Where an AO authorises such an investigation or operation the Central Record of Authorisations should highlight this, and it should be brought to the attention of the Inspector during their next inspection.

8.12 The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 prescribes that for the Council, the AO shall be a Director, Head of Service, Service Manager or equivalent as distinct from the Officer responsible for the conduct of an investigation.

8.13 A designated AO must qualify both by rank and by competence. Officers who wish to be designated must have been trained to an appropriate level in order to have an understanding of RIPA and the requirements that must be satisfied before an authorisation can be granted.

8.14 Authorisations must be given in writing by the AO by completing the relevant section on the authorisation form. Before giving authorisation for directed surveillance, an AO must be satisfied that the reason for the request is for the prevention and detection of crime and that the crime attracts a custodial sentence of a maximum of 6 months or more, or is an offence relating to the underage sale of alcohol or tobacco under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933.

8.15 The lawful criteria for CHIS are prevention and detection of crime and prevention of disorder and the offence does not have to have a sentence of 6 months imprisonment but consideration must be given to the risk of collateral intrusion (the risk of obtaining private information about persons who are not the subject of investigation), the possibility of collecting confidential personal information and that the result cannot reasonably be achieved by any other means.

8.16 When completing an authorisation, the case should be presented in a fair and balanced way. In particular, all reasonable efforts should be made to take into account information which weakens the case for the authorisation.

8.17 The application should explain why the activity is both necessary and proportionate, having regard to the collateral intrusion. It should also explain exactly what is being authorised, against whom, in what circumstances, where and so on, and that the level of the surveillance is appropriate to achieve the

objectives. It is important that this is very clear as the surveillance operatives will only be able to carry out activity that has been authorised. This will assist with avoiding errors.

8.18 If any equipment such as covert cameras are to be used, the AO should know the capability of the equipment before authorising its use. This will have an impact on collateral intrusion, necessity and proportionality. It is important that they consider all the facts to justify their decision and that it is not merely a rubber-stamping exercise.

8.19 The AO may be required to attend court to explain what has been authorised and why. Alternatively, they may have to justify their actions at a tribunal. AOs are also responsible for carrying out regular reviews of applications, for authorising renewals and cancelling any authorisation (see relevant sections below).

8.20 AOs must acquaint themselves with the relevant Codes of Practice issued by the Home Office regarding RIPA and the current Procedures and Guidance issued by the Commissioner. This document also details the latest operational guidance to be followed. It is recommended that AOs hold their own copy of this document.

8.21 AOs, through the Council's Data Controller, must ensure compliance with the appropriate data protection requirements under data protection legislation and regulation and any relevant internal protocols of the Council relating to the handling and storage of material.

9. SURVEILLANCE TYPES AND CRITERIA

9.1 Surveillance is:

- Monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications.
- Recording anything monitored, observed or listened to in the course of surveillance, with or without the assistance of a device.

9.2 By its very nature, surveillance may involve invading an individual's right to privacy. The level of privacy which individuals can expect depends upon the nature of the environment they are within at the time. For example, within an individual's own home or private vehicle, an individual can expect the highest level of privacy. The level of expectation of privacy may reduce if the individual transfers out into public areas.

9.3 There are different types of surveillance which, depending on their nature, are either allowable or not allowable and that require different degrees of authorisation and monitoring under RIPA.

9.4 OVERT SURVEILLANCE

9.5 Overt surveillance is where the subject of surveillance is aware that it is taking place. This could be by way of signage, such as in the use of CCTV, or because the subject of the surveillance has been informed of the activity. Overt surveillance is outside the scope of RIPA and therefore does not require authorisation. However, it still must take account of privacy under the HRA.

9.6 COVERT SURVEILLANCE

9.7 Covert Surveillance is defined as "surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that

it is or may be taking place" and is covered by RIPA. Covert surveillance is categorised as either intrusive or directed.

9.8 There are three categories of covert surveillance regulated by RIPA:

1) **Directed Surveillance;**

2) **Covert Human Intelligence Sources** (CHIS); and

3) **Intrusive surveillance** (the Council is not permitted to carry out intrusive surveillance).

9.9 INTRUSIVE SURVEILLANCE

9.10 The Council has no authority in law to carry out Intrusive Surveillance. Intrusive surveillance is defined in section 26(3) of RIPA as covert surveillance that:

- Is carried out in relation to anything taking place on any residential premises or in any private vehicle; and
- Involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

9.11 Where surveillance is carried out in relation to anything taking place on any residential premises or in any private vehicle by means of a device, without that device being present on the premises, or in the vehicle, it is not intrusive unless the device consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle. Thus, an observation post outside premises, which provides a limited view and no sound of what is happening inside the premises, would not be considered as intrusive surveillance.

9.12 A risk assessment of the capability of equipment being used for surveillance of residential premises and private vehicles should be carried out to ensure that it does not fall into intrusive surveillance.

9.13 If you are considering conducting surveillance that may fall within the scope of intrusive surveillance you must contact the RIPA Coordinator for clarification or seek legal advice from the legal department before you undertake any surveillance.

9.14 DIRECTED SURVEILLANCE

9.15 Surveillance is directed surveillance within RIPA if the following are applicable:

- It is covert, but not intrusive surveillance;
- It is conducted for the purposes of a specific investigation or operation;
- It is likely to result in the obtaining of private information (see private information below) about a person (whether or not one specifically identified for the purposes of the investigation or operation);
- It is conducted otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation to be sought.
- The offence under investigation attracts a maximum custodial sentence of six months, or it is an investigation into criminal offences relating to the underage sale of alcohol or tobacco under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933.

10. PRIVATE INFORMATION

10.1 The Code of Practice provides guidance on the definition of private information and states it includes any information relating to a person's private or family life. As a result, private information is capable of comprising any aspect of a person's relationship with others including family and professional or business relationships.

10.2 Information which is non-private may include publicly available information such as books, newspapers, journals, TV and radio broadcasts, newswires, web sites, mapping imagery, academic articles, conference proceedings, business reports, and more. Such information may also include commercially available data where a fee may be charged, and any data which is available on request or made available at a meeting to a member of the public.

10.3 Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public, and where a record is being made by the Council of that person's activities for future consideration or analysis.

10.4 Surveillance of publicly accessible areas of the internet should be treated in a similar way particularly when accessing information on social media websites. (See the Internet and Social Media Research and Investigations Policy for further guidance)

10.5 Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish a pattern of behaviour. Consideration must be given if one or more pieces of information (whether or not available in the public domain) are covertly and / or overtly obtained for the purpose of making a permanent record about a person or for subsequent data processing to generate further information. In such circumstances, the totality of information gleaned may constitute private information even if individual records do not. Where such conduct includes covert surveillance, a directed surveillance authorisation may be considered appropriate.

10.6 Private information may include personal data, such as names, telephone numbers and address details. Where such information is acquired by means of covert surveillance of a person having a reasonable expectation of privacy, a directed surveillance authorisation is appropriate

11. CONFIDENTIAL OR PRIVILEGED MATERIAL

11.1 Particular consideration should be given in cases where the subject of the investigation or operation might reasonably assume a high degree of confidentiality. This includes where the material contains information that is legally privileged; confidential journalistic material or where material identifies a journalist's source; or material containing confidential personal information or communications between a Member of Parliament and another person on constituency business. Directed surveillance likely or intended to result in the acquisition of knowledge of confidential or privileged material must be authorised by the Head of Paid Service, or (in their absence) the person acting as the Head of Paid Service (as per the codes and Statutory Instrument). Advice should be sought from the RIPA Coordinator and the Legal Department if there is a likelihood of this occurring.

12. INTERNET AND SOCIAL MEDIA INVESTIGATIONS

12.1 Online open source research is widely regarded as the collection, evaluation and analysis of material from online sources available to the public, whether by payment or otherwise to use as intelligence and evidence.

12.2 The use of online open source internet and social media research techniques has become a productive method of obtaining information to assist the Council with its regulatory and enforcement functions. It can also assist with service delivery issues and debt recovery. However, the use of the internet and social media is constantly evolving and with it the risks associated with these types of enquiries, particularly regarding breaches of privacy under Article 8 Human Rights Act (HRA) and other operational risks. The activity may also require RIPA authorisations for Directed Surveillance or CHIS. Where this is the case, the application process and the contents of this policy are to be followed.

12.3 There is a detailed Internet and Social Media Research and Investigations Policy that covers online open source research which should be read and followed in conjunction with this policy.

13. CCTV

13.1 The use of the CCTV systems operated by the Council does not normally fall under the RIPA regulations. However, it does fall under the data protection legislation and regulations, the Surveillance Camera Code 2013 and the Council's CCTV Policy. However, should there be a requirement for the CCTV cameras to be used for a specific purpose to conduct surveillance it is likely that the activity will fall under directed surveillance and therefore require an authorisation under RIPA. The Council's CCTV Policy and Procedures should be referred to.

13.2 If an IO envisages using any other CCTV system they should contact the RIPA Coordinator concerning any clarification on the administrative process or seek legal advice before they undertake any surveillance.

14. AUTOMATIC NUMBER PLATE RECOGNITION (ANPR)

14.1 Automated Number Plate Recognition (ANPR) does not engage RIPA if it is used for the purpose it is registered for, such as traffic flow management or safety and enforcement within car parks. However, it is capable of being a surveillance device if used in a pre-planned way to carry out surveillance by monitoring a particular vehicle or by plotting its locations, e.g. in connection with illegally disposing of waste.

14.2 Should it be necessary to use the Police ANPR systems to monitor vehicles, the same RIPA principles apply regarding when a directed surveillance authorisation should be sought.

15. JOINT AGENCY SURVEILLANCE

15.1 In cases where one agency is acting on behalf of another, it is usually for the tasking agency to obtain or provide the authorisation. For example, where surveillance is carried out by Council employees on behalf of the Police, authorisation would be sought by the Police. If it is a joint operation involving both agencies, the lead agency should seek authorisation.

15.2 Council staff involved with joint agency surveillance must ensure that all parties taking part are authorised on the form to carry out the activity. When Council Officers are operating on another organisation's authorisation they are to ensure they see what activity they are authorised to carry out and make a written record. They should also provide a copy of the authorisation to the RIPA Coordinator at the Council to assist with oversight and monitoring.

16. USE OF THIRD PARTY AGENTS

16.1 In some circumstances it may be appropriate or necessary for the Council to work with third parties who are not themselves a public Authority (such as an individual, company or non-governmental organisation) to assist with an investigation. Where that third party is acting in partnership with or under the direction of the Council, then they are acting as our agent and any activities that the third party conducts which meet the RIPA definitions of directed surveillance should be authorised. The agent will be subject to RIPA in the same way as any employee of the Council would be. The AO should ensure that the agents are qualified or have the necessary skills to achieve the objectives. They should also ensure that they understand their obligations under RIPA. If advice is required, please contact the Legal Department.

16.2 If the above circumstances apply and it is intended to instruct an agent to carry out the covert activity, the agent must complete and sign the appropriate form.

16.3 Similarly, a surveillance authorisation should also be considered where the Council is aware that a third party (that is not a public Authority) is independently conducting surveillance and the Council intends to make use of any suitable material obtained by the third party for the purposes of a specific investigation or is to act as the prosecuting body.

17. EQUIPMENT

17.1 All equipment capable of being used for directed surveillance, such as cameras, should be fit for the purpose for which they are intended. The equipment should be logged on the central register of equipment held by the RIPA Coordinator. This will require a description, Serial Number, and an explanation of its capabilities.

17.2 When completing an Authorisation, the applicant must provide the AO with details of any equipment to be used and its technical capabilities. The AO will have to take this into account when considering the intrusion issues and proportionality. The AO must make it clear on the Authorisation exactly what equipment, if any, they are authorising and under what circumstances.

18. COVERT HUMAN INTELLIGENCE SOURCES (CHIS)

18.1 This policy applies to all use of under-cover Officers or informants, referred to as Covert Human Intelligence Sources (CHIS). Not all human source activity will meet the definition of a CHIS. For example, a source may be a public volunteer or someone who discloses information out of a professional or statutory duty or has been tasked to obtain information other than by way of a covert relationship.

18.2 Test purchase activity does not in general require authorisation under RIPA as vendor-purchaser activity does not constitute a relationship. However, if a number of visits are undertaken, a relationship may be established and

authorisation as a CHIS should be considered. Equally a test purchase may meet the definition of directed surveillance.

18.3 If you intend to instruct a third party to act as the CHIS, the agent must complete and sign the appropriate form. The agent will be subject to RIPA in the same way as any employee of the Council would be. If advice is required, please contact either the RIPA Coordinator or the Legal Department.

18.4 An application for either directed surveillance or the use of a CHIS will need authorising internally by an AO. If authorised by the AO, approval will be required from a Justice of the Peace (JP) prior to any activity taking place. (See the appropriate sections below).

18.5 The authorisation request should be accompanied by a risk assessment, giving details of how the CHIS is going to be handled and the arrangements which are in place for ensuring that there is at all times a person with responsibility for maintaining a record of the use made of CHIS. The risk assessment should take into account the safety and welfare of the CHIS in relation to the activity and should consider the likely consequences should the role of the CHIS become known. The ongoing security and welfare of the CHIS after the cancellation of the authorisation should also be considered at the outset.

18.6 Where surveillance or the use of a CHIS is likely to result in the obtaining of confidential information, it is imperative that legal advice should first be sought from the SRO or the Legal Department. Confidential information includes, though is not limited to, matters subject to legal privilege, confidential personal information and confidential journalistic material. Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling concerning an individual (whether living or dead) who can be identified from it.

18.7 Should a CHIS authority be required, all of the staff involved in the process should make themselves fully aware of all of the aspects relating to tasking contained within the CHIS codes of Practice.

18.8 Legal advice should always be sought where consideration is given to the use of CHIS.

18.9 DEFINITION OF CHIS

18.10 A CHIS is a person who: -

- Establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within the following paragraphs;
- Covertly uses such a relationship to obtain information or to provide access to any information to another person; or
- Covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

18.11 A relationship is established, maintained or used for a covert purpose if, and only if, it is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

18.12 The serious crime criteria of the offences under investigation do not apply to CHIS.

18.13 CHIS's may only be authorised if the following arrangements are in place:

- That there will at all times be an Officer (the handler) within the Council who will have day to day responsibility for dealing with the source on behalf of the authority, and for the source's security. The handler is likely to be the IO,
- That there will at all times be another Officer within the Council who will have general oversight of the use made of the source; (controller) i.e. the Line Manager.
- That there will at all times be an Officer within the Council who has responsibility for maintaining a record of the use made of the source.
- That the records relating to the source maintained by the local authority will always contain particulars of all matters specified by the Secretary of State in Regulations.

18.14 The Handler will have day to day responsibility for:

- dealing with the source on behalf of the Council concerned;
- directing the day to day activities of the source;
- recording the information supplied by the source; and
- monitoring the source's security and welfare.

18.15 The Controller will be responsible for the general oversight of the use of the source.

18.16 Tasking is the assignment given to the source by the Handler or Controller such as asking them to obtain information, to provide access to information or to otherwise act, incidentally, for the benefit of the relevant Council. Authorisation for the use or conduct of a source is required prior to any tasking where such tasking requires the source to establish or maintain a personal or other relationship for a covert purpose.

18.17 In some instances, the tasking given to a person will not require the source to establish a personal or other relationship for a covert purpose. For example, a member of the public is asked to maintain a record of all vehicles arriving and leaving a specific location or to record the details of visitors to a neighbouring house. A relationship has not been established or maintained in order to gather the information and a CHIS authorisation is therefore not available. Other authorisations under the Act, for example, directed surveillance, may need to be considered where there is a possible interference with the Article 8 rights of an individual.

18.18 Authorisations should not be drawn so narrowly that a separate authorisation is required each time the CHIS is tasked. Rather, an authorisation might cover, in broad terms, the nature of the source's task.

18.19 VULNERABLE CHIS

18.20 Special consideration must be given to the use of a Vulnerable Individual as a CHIS. A 'Vulnerable Individual' is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself, or unable to protect himself against significant harm or exploitation. Any individual of this description, or a Juvenile as defined below, should only be authorised to act as a source in the most exceptional circumstances and only then when authorised by the by the Head of Paid Service, or (in their absence) the person acting as the Head of Paid Service (as per the codes and Statutory Instrument).

18.21 Special safeguards also apply to the use or conduct of Juvenile Sources; that is sources under the age of 18 years. On no occasion should the use or conduct of a source under 16 years of age be authorised to give information against his parents or any person who has parental responsibility for them.

18.22 If the use of a Vulnerable Individual or a Juvenile is being considered as a CHIS you must consult the Legal Department before authorisation is sought as authorisations should not be granted unless the special provisions contained within the Regulation of Investigatory Powers (Juveniles) Order 2000; SI No. 2793 are satisfied. Authorisations for Juvenile Sources must be authorised by the by the Head of Paid Service, or (in their absence) the person acting as the Head of Paid Service (as per the codes and Statutory Instrument).

18.23 It is unlikely that the use of a Vulnerable Individual or Juvenile CHIS by the Council will meet the requirements of necessity and proportionality and be considered justifiable.

18.24 USE OF EQUIPMENT BY A CHIS

18.25 If a CHIS is required to wear or carry a surveillance device such as a covert camera it does not need a separate intrusive or directed surveillance authorisation, provided the device will only be used in the presence of the CHIS. It should be authorised as part of the conduct of the CHIS.

18.26 CHIS, whether or not wearing or carrying a surveillance device, in residential premises or a private vehicle, does not require additional authorisation to record any activity inside those premises or that vehicle which takes place in their presence. This also applies to the recording of telephone conversations.

18.27 CHIS MANAGEMENT

18.28 The operation will require managing by the handler and controller which will include ensuring that the activities of the source and the operation remain focused and there is no status drift. It is important that the intrusion is assessed on an ongoing basis to ensure the operation remains proportionate. The security and welfare of the source will also be monitored. The AO should maintain general oversight of these functions.

18.29 During CHIS activity there may be occasions when unforeseen action or undertakings occur. Such incidences should be recorded as soon as practicable after the event and if the existing authorisation is insufficient, it should either be dealt with by way of a review and updated (for minor amendments only) or it should be cancelled, and a new authorisation obtained before any further action is carried out. Similarly, where it is intended to task a CHIS in a new significantly different way than previously identified, the proposed tasking should be referred to the AO, who should consider whether a separate authorisation is required. This should be done in advance of any tasking and details of such referrals must be recorded.

18.30 CHIS RECORD KEEPING

18.31 The records relating to the source maintained by the Council will always contain particulars as laid down by the Covert Human Intelligence Sources codes of practice, revised CHIS codes of practice and the RIPA (Source Records) Regulations 2000; SI No: 2725 which details the particulars that must be included in these records.

19. NECESSITY

19.1 Obtaining an authorisation under RIPA will only ensure that there is a justifiable interference with an individual's Article 8 rights if it is necessary and proportionate for these activities to take place.

19.2 RIPA first requires that the person granting an authorisation believe that the authorisation is necessary in the circumstances of the particular case for one or more of the statutory grounds applicable to the Council.

19.3 The applicant must be able to demonstrate why it is necessary to carry out the covert activity to achieve the objectives and that there was no other means of obtaining the same information in a less intrusive method. The applicant must detail the crime being investigated and the information or evidence they are hoping to obtain. They should also state that they have considered other means of obtaining this information and have either concluded this is the only method available or that other methods are not appropriate and state the reason; for example it would alert the subject to their investigation which would be detrimental to the case.

20. PROPORTIONALITY

20.1 If the activities are deemed necessary, the AO must also believe that they are proportionate to the objective they are aiming to achieve. This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms.

20.2 The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render the proposed actions proportionate. Similarly, an offence may be so minor that any deployment of covert techniques would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

20.3 When completing the authorisation the AO should explain why the methods and tactics to be adopted during the surveillance are justified in the particular circumstances of the case.

20.4 The Codes provide guidance relating to proportionality which should be considered by both applicants and AOs:

- Balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- Explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- Considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- Evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

20.5 When completing an application for authorisation, the case should be presented in a fair and balanced way. In particular, all reasonable efforts should be made to take into account information which weakens the case for the authorisation.

21. COLLATERAL INTRUSION

21.1 Before authorising applications for directed surveillance, the AO should also take into account the risk of collateral intrusion - obtaining private information about persons who are not subjects of the surveillance.

21.2 Officers should take measures, wherever practicable, to avoid or minimise unnecessary intrusion into the privacy of those who are not the intended subjects of the surveillance. Where such collateral intrusion is unavoidable, the activities may still be authorised, provided this intrusion is considered proportionate to the aims of the operation. The same proportionality tests apply to anticipated collateral intrusion as to intrusion into the privacy of the intended subject of the surveillance.

21.3 All applications must include an assessment of the risk of collateral intrusion and details of any measures taken to limit this (within the relevant section of the form), to enable the AO to fully consider the proportionality of the proposed actions.

21.4 In order to give proper consideration to collateral intrusion, an AO should be given full information regarding the potential scope of the anticipated surveillance, including the likelihood that any equipment or software deployed may cause intrusion on persons or property other than the subject(s) of the application. If an automated system such as an online search engine is used to obtain the information, the AO should be made aware of its potential extent and limitations. Material which is not necessary or proportionate to the aims of the operation or investigation should be discarded or securely retained separately where it may be required for future evidential purposes. The AO should ensure appropriate safeguards for the handling, retention or destruction of such material, as well as compliance with Data Protection Act requirements.

21.5 Where it is proposed to conduct surveillance activity specifically against individuals who are not suspected of direct or culpable involvement in the overall matter being investigated, interference with the privacy of such individuals should not be considered as collateral intrusion but rather as intended intrusion.

21.6 Where the Council intends to access a social media or other online account to which they have been given access with the consent of the owner, the authority will still need to consider whether the account(s) may contain information about others who have not given their consent. If there is a likelihood of obtaining private information about others, the need for a Directed Surveillance authorisation should be considered, particularly (though not exclusively) where it is intended to monitor the account going forward.

22. THE APPLICATION AND AUTHORISATION PROCESS

22.1 All forms relating to RIPA can be found at https://www.gov.uk/government/collections/ripa-forms--2

22.2 DURATION OF AUTHORISATIONS

22.3 Authorisations must be given for the maximum duration from the date approved by the JP/Magistrate but reviewed on a regular basis and formally cancelled when no longer needed. Authorisations should not be allowed to simply expire – they must be cancelled when the surveillance is no longer proportionate or necessary. Therefore, a directed surveillance authorisation will cease to have effect after three months from the date of approval by the Magistrate unless renewed or cancelled. Durations detailed below:

- Directed Surveillance 3 Months
- Renewal 3 Months
- Covert Human Intelligence Source 12 Months
- Renewal 12 months
- Juvenile Sources 4 Months
- Renewal 4 Months

22.4 It is the responsibility of the IO to make sure that the authorisation is still valid when they undertake surveillance.

22.5 APPLICATIONS/AUTHORISATION

22.6 The applicant must carry out a feasibility study and intrusion assessment as this may be required by the AO. The person seeking the authorisation should then complete the application form having regard to the guidance given in this Policy and the statutory Codes of Practice. There should not be any real delay between the feasibility study and the completion of the application form to ensure that the details within the application remain accurate. The form should then be submitted to the AO for authorisation.

22.7 When completing an application, the applicant must ensure that the case for the authorisation is presented in a fair and balanced way. In particular, all reasonable efforts should be made to take into account information which weakens the case for the warrant or authorisation.

22.8 For directed surveillance, the offence must be a criminal offence that attracts a maximum custodial sentence of six months or more or criminal offences relating to the underage sale of alcohol or tobacco under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933.

22.9 All the relevant sections must be completed with enough information to ensure that applications are sufficiently detailed for the AO to consider necessity and proportionality, having taken into account the collateral intrusion issues. AOs should refuse to authorise applications that are not to the required standard and should refer them back to the originating Officers. Cutting and pasting or using template entries should not take place as this would leave the process open to challenge.

22.10 If it is intended to undertake both directed surveillance and the use of a CHIS on the same surveillance subject, the respective application form and procedures should be followed, and both activities should be considered separately on their own merits.

22.11 All applications will be submitted to the AO via the Line Manager of the appropriate enforcement team in order that they are aware of the application and activities being undertaken by their staff. The Line Manager will perform an initial quality check of the application. However, they should not be involved in the sanctioning of the authorisation.

22.12 Applications, whether authorised or refused, will be issued with a unique number (obtained from the RIPA Coordinator) by the AO, taken from the next available number in the central record of authorisations which is held by the RIPA Coordinator.

22.13 If not authorised, feedback will be provided to the applicant and the application will be forwarded to the RIPA Coordinator for recording and filing.

22.14 If authorised, the applicant will then complete the relevant section of the judicial application/order form. Although this form requires the applicant to provide a

brief summary of the circumstances of the case, this is supplementary and does not replace the need to supply the original RIPA authorisation form to the Court.

22.15 ARRANGING THE COURT HEARING

22.16 Within office hours a hearing must be arranged at the Magistrates' Court with Her Majesty's Courts and Tribunals Service (HMCTS). The hearing will be in private and heard by a single JP. The application to the JP will be on oath.

22.17 Officers who may present the application at these proceedings will need to be formally designated by the Council under section 223 of the Local Government Act 1972 to appear, be sworn in and present evidence or information as required by the JP. The legal department can advise who is duly authorised and able to present.

22.18 ATTENDING THE HEARING

22.19 The applicant and the AO should attend the Hearing to answer any questions directed at them. Upon attending the hearing, the presenting Officer must provide to the JP the partially completed judicial application/order form, a copy of the RIPA application/authorisation form, and the original form, together with any supporting documents setting out the case.

22.20 The original RIPA authorisation should be shown to the JP but will be retained by the Council so that it is available for inspection by IPCO, and in the event of any legal challenge or investigations by the IPT.

22.21 The JP will read and consider the RIPA authorisation and the judicial application/order form. They may ask questions to clarify points or require additional reassurance on particular matters. These questions are supplementary to the content of the application form**.** The forms and supporting papers must by themselves make the Council's case. It is not sufficient for the Council to provide oral evidence where this is not reflected or supported in the papers provided.

22.22 The JP will consider whether they are satisfied that at the time the authorisation was granted or renewed, there were reasonable grounds for believing that the authorisation was necessary and proportionate. In addition, they must be satisfied that the person who granted the authorisation or gave the notice was an appropriate Designated Person within the Council and the authorisation was made in accordance with any applicable legal restrictions, for example that the crime threshold for directed surveillance has been met.

22.23 DECISION OF THE JP

22.24 The JP has a number of options:

22.25 Approve or renew an authorisation. If approved by the JP, the date of the approval becomes the commencement date and the three months duration will commence on this date, the Officers are now allowed to undertake the activity.

22.26 Refuse to approve or renew an authorisation. The RIPA authorisation will not take effect and the Council may **not** use the technique in that case.

22.27 Where an application has been refused, the applicant may wish to consider the reasons for that refusal. If more information was required by the JP to determine whether the authorisation has met the tests, and this is the reason for refusal, the Officer should consider whether they can reapply. For example, if there was

information to support the application which was available to the Council, but not included in the papers provided at the hearing.

22.28 For, a technical error (as defined by the JP), the form may be remedied without going through the internal authorisation process again. The Officer may then wish to reapply for judicial approval once those steps have been taken.

22.29 Refuse to approve or renew and quash the authorisation. This applies where the JP refuses to approve or renew the authorisation and decides to quash the original authorisation. However, the court must not exercise its power to quash the authorisation unless the applicant has had at least two business days from the date of the refusal in which to make representations. If this is the case the Officer will inform the Legal Department who will consider whether to make any representations.

22.30 The JP will record their decision on the order section of the judicial application/order form. The court administration will retain a copy of the Council's RIPA application and authorisation form and the judicial application/order form. The Officer will retain the original authorisation and a copy of the judicial application/order form.

22.31 The Council may only appeal a JP decision on a point of law by judicial review. If such a concern arises, the Legal Department will decide what action if any should be taken.

22.32 POST COURT PROCEDURE

22.33 It will be necessary to work out the cancellation date from the date of approval and ensure that the applicant and the AO are aware. The original application and the copy of the judicial application/order form should be forwarded to the RIPA Coordinator. A copy will be retained by the applicant and if necessary by the AO. The Central Register of Authorisations will be updated with the relevant information to comply with the Codes of Practice and the original documents filed and stored securely.

22.34 Where dates are set within the process such as reviews, they must be adhered to. This will help with demonstrating that the process has been managed correctly in line with the Codes of Practice.

22.35 MANAGEMENT OF THE ACTIVITY

22.36 All RIPA activity will need to be managed by all the persons involved in the process. It is important that all those involved in undertaking directed surveillance activities are fully aware of the extent and limits of the authorisation. There should be an ongoing assessment of the need for the continued activity, including ongoing assessments of the intrusion. All material obtained including evidence should be stored in line with relevant legislation and procedures to safeguard its integrity and reduce a risk of challenge. (See use of material as evidence**)**

22.37 REVIEWS

22.38 When an application has been authorised and approved by a JP, regular reviews must be undertaken by the AO to assess the need for the surveillance to continue.

22.39 In each case the AO should determine at the outset how often a review should take place. This should be as frequently as is considered necessary and

practicable. Particular attention is drawn to the need to review authorisations frequently where the surveillance provides a high level of intrusion into private life or significant collateral intrusion, or may obtain confidential information. Review periods will be recorded on the application form and the decision will be based on the circumstances of each application. However, reviews should be conducted at least monthly to ensure that the activity is managed. It will be important for the AO to be aware of when reviews are required following an authorisation, to ensure timely submission of the review form.

22.40 Applicants are responsible for submitting a review form by the date set by the AO. They should also use a review form for any changes in circumstances to the original application which would comprise a change to the level of intrusion so that the requirement to continue the activity can be reassessed. The applicant does not have to wait until the review date if it is being submitted for a change in circumstances. If the circumstances or the objectives have changed considerably, or the techniques to be used are now different, a new RIPA application form should be submitted and the process followed to obtain approval by a JP.

22.41 Line managers should also make themselves aware of the required review periods to ensure that the relevant forms are completed on time.

22.42 The reviews are dealt with internally by submitting the review form to the AO. There is no requirement for a review form to be submitted to a JP.

22.43 The results of a review should be recorded on the Central Record of Authorisations.

22.44 RENEWAL

22.45 A renewal form is to be completed by the applicant when the original authorisation period is about to expire but directed surveillance or the use of a CHIS is still required.

22.46 Renewals must be approved by a JP.

22.47 Applications for renewals should not be made until shortly before the original authorisation period is due to expire but the applicant must take account of factors which may delay the renewal process (e.g. intervening weekends or the availability of the relevant AO and a JP to consider the application).

22.48 The applicant should complete all the sections within the renewal form and submit the form to the AO for consideration.

22.49 AOs should examine the circumstances with regard to necessity, proportionality and the collateral intrusion issues before making a decision to renew the activity. A CHIS application should not be renewed unless a thorough review has been carried out covering the use made of the source, the tasks given to them and information obtained. The AO must consider the results of the review when deciding whether to renew or not. The review and the consideration must be documented.

22.50 If the AO refuses to renew the application, the cancellation process should be completed. If the AO authorises the renewal of the activity, the same process is to be followed as for the initial application whereby approval must be sought from a JP.

22.51 A renewal takes effect on the day on which the authorisation would have ceased and lasts for a further period of three months.

22.52 CANCELLATION

22.53 The cancellation form is to be submitted by the applicant or another investigator in their absence. The AO who granted or last renewed the authorisation must cancel it if they are satisfied that the directed surveillance no longer meets the criteria upon which it was authorised. Where the AO is no longer available, this duty will fall on the person who has taken over the role of AO or the person who is acting as AO.

22.54 As soon as the decision is taken that directed surveillance should be discontinued, the applicant or other IO involved in the investigation should inform the AO. The AO will formally instruct the IO to cease the surveillance, noting the time and date of their decision. This will be required for the cancellation form. The date and time when such an instruction was given should also be recorded in the Central Record of Authorisations**.**

22.55 The IO submitting the cancellation should complete in detail the relevant sections of the form and include the period of surveillance and also detail if any images were obtained, particularly any images containing third parties. The AO should then take this into account and issue instructions regarding the management and disposal of the images. See section below; Safeguarding and the Use of Surveillance Material.

22.56 The cancellation process should also be used to evaluate whether the objectives have been achieved and whether the applicant acted within the authorisation. This check will form part of the oversight function. Where issues are identified, they will be brought to the attention of the Line Manager and the SRO.

22.57 When cancelling a CHIS authorisation an assessment of the welfare and safety of the source should be assessed, and any issues identified and reported as above.

23. SURVEILLANCE OUTSIDE OF RIPA

23.1 As previously detailed, amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 mean that Councils can now only grant an authorisation under RIPA where the Council is investigating criminal offences which attract a maximum custodial sentence of at least six months or criminal offences relating to the underage sale of alcohol or tobacco.

23.2 As a result of the changes in legislation, it is envisaged that surveillance may be required which falls outside of RIPA (for example in the case of anti-social behaviour disorders which do not attract a maximum custodial sentence of at least six months imprisonment).

23.3 As stated, conducting surveillance outside of RIPA is not fundamentally unlawful, however in order for the Council to defend claims that they have breached an individual's right to privacy under the HRA the Council needs to demonstrate that their actions were justified in the circumstances of the case. It is therefore the Council's policy that, in order to undertake surveillance that falls outside of RIPA, Officers will follow the same initial process as when they are making an application for authorisation under RIPA. The IO must complete a Non-RIPA application form that is authorised by an AO and the application will be lodged with and monitored by the RIPA Coordinator. The AO will need to be satisfied that the actions are necessary and proportionate and give due consideration to any collateral intrusion. The Non-RIPA authorisation form is available from the RIPA Coordinator. The procedure for review and renewal of the surveillance

application will be the same, however there is no requirement/ability to obtain authorisation from a JP.

23.4 Non-RIPA surveillance also includes staff surveillance in serious disciplinary investigations. Any surveillance of staff must be formally recorded on the Non-RIPA surveillance application form and authorised by the AO in consultation with the RIPA Coordinator. The review of staff usage of the internet and e-mail would also not fall under RIPA. This surveillance outside of RIPA must however be compliant with any Council Policies with regard to monitoring at work and business practices legislation and should also consider ICO guidance in relation to surveillance of staff. Surveillance of staff should only be carried out in exceptional circumstances.

23.5 The RIPA codes also provide guidance that authorisation under RIPA is not required for the following types of activity:

- General observations that do not involve the systematic surveillance of an individual or a group of people and should an incident be witnessed the Officer will overtly respond to the situation.
- Use of overt CCTV and Automatic Number Plate Recognition systems.
- Surveillance where no private information is likely to be obtained.
- Surveillance undertaken as an immediate response to a situation.
- Covert surveillance not relating to criminal offence which carries a maximum sentence of 6 months imprisonment and does not relate to the sale of alcohol or tobacco to children (surveillance outside of RIPA).
- The use of a recording device by a CHIS in respect of whom an appropriate use or conduct authorisation has been granted permitting them to record any information in their presence.
- The covert recording of noise where the recording is of decibels only or constitutes non-verbal noise (such as music, machinery or an alarm), or the recording of verbal content is made at a level which does not exceed that which can be heard from the street outside or adjoining property with the naked ear. In the latter circumstance, the perpetrator would normally be regarded as having forfeited any claim to privacy. In either circumstance this is outside of RIPA.

24. SAFEGUARDING AND THE USE OF SURVEILLANCE MATERIAL

24.1 This section provides guidance on the procedures and safeguards to be applied in relation to the handling of any material obtained through directed surveillance or CHIS activity. This material may include private, confidential or legally privileged information.

24.2 AUTHORISED PURPOSE

24.3 Dissemination, copying and retention of material must be limited to the minimum necessary for authorised purposes (for CHIS activity, this is 5 years and for surveillance activity, this is 3 years). For the purposes of the Code this is defined as follows:-

- It is, or is likely to become, necessary for any of the statutory purposes set out in the RIPA in relation to covert surveillance or CHIS activity;

- It is necessary for facilitating the carrying out of the functions of public authorities under RIPA;
- It is necessary for facilitating the carrying out of any functions of the Commissioner or the Investigatory Powers Tribunal;
- It is necessary for the purposes of legal proceedings; or
- It is necessary for the performance of the functions of any person by or under any enactment.

24.1 USE OF MATERIAL AS EVIDENCE

24.2 Material obtained through directed surveillance, may be used as evidence in criminal proceedings. The admissibility of evidence is governed primarily by the common law, the Criminal Procedure and Investigations Act 1996 (CPIA), the Civil Procedure Rules, section 78 of the Police and Criminal Evidence Act 1984 and the Human Rights Act 1998.

24.3 Ensuring the continuity and integrity of evidence is critical to every prosecution. Accordingly, considerations as to evidential integrity are an important part of the disclosure regime under the CPIA and these considerations will apply to any material acquired through covert surveillance that is used in evidence. When information obtained under a covert surveillance authorisation is used evidentially, the Council must be able to demonstrate how the evidence has been obtained, to the extent required by the relevant rules of evidence and disclosure.

24.4 Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements. In a criminal case the codes issued under CPIA will apply. They require that the investigator record and retain all relevant material obtained in an investigation and later disclose relevant material to the prosecuting solicitor. They in turn will decide what is disclosed to the defence solicitor.

24.5 There is nothing in RIPA which prevents material obtained under directed or intrusive surveillance authorisations from being used to further other investigations.

24.6 HANDLING AND RETENTION OF MATERIAL

24.7 All material associated and obtained with an application will be subject to the provisions of all data protection legislation and regulations and CPIA Codes of Practice and to any Council Policies with regard to data retention and security. All Officers involved within this process should make themselves aware of the provisions within this legislation and how it impacts on the RIPA process. Material obtained together with relevant associated paperwork should be held securely. Extra care needs to be taken if the application and material relates to a CHIS.

24.8 Material required to be retained under CPIA should be retained until a decision is taken whether to institute proceedings against a person for an offence or if proceedings have been instituted, at least until the accused is acquitted or convicted or the prosecutor decides not to proceed with the case.

24.9 Where the accused is convicted, all material which may be relevant must be retained at least until the convicted person is released from custody, or six months from the date of conviction, in all other cases.

24.10 If the court imposes a custodial sentence and the convicted person is released from custody earlier than six months from the date of conviction, all material which may be relevant must be retained at least until six months from the date of conviction.

24.11 If an appeal against conviction is in progress when the convicted person is released, or at the end of the period of six months, all material which may be relevant must be retained until the appeal is determined.

24.12 Retention beyond these periods must be justified under data protection legislation and regulations. AOs, through the Council's Data Controller, must ensure compliance with the appropriate Data Protection requirements and any relevant internal arrangements produced by the Council relating to the handling and storage of material.

24.13 DISSEMINATION OF INFORMATION

24.14 It may be necessary to disseminate material acquired through the RIPA covert activity within the Council or with other Councils or agencies, including the Police. The number of persons to whom any of the information is disclosed, and the extent of disclosure, should be limited to the minimum necessary. It must also be in connection with an authorised purpose as set out above. It will be necessary to consider exactly what and how much information should be disclosed. Only so much of the material may be disclosed as the recipient needs; for example, if a summary of the material will suffice, no more than that should be disclosed.

24.15 The obligations apply not just to the Council as the original authority acquiring the information, but also to anyone to whom the material is subsequently disclosed. In some cases, this will be achieved by requiring the latter to obtain permission from the Council before disclosing the material further. It is important that the Officer in Charge (OIC) of the enquiry considers these implications at the point of dissemination to ensure that safeguards are applied to the data.

24.16 A record will be maintained justifying any dissemination of material. If in doubt, seek legal advice.

24.17 STORAGE

24.18 Material obtained through covert surveillance, and all copies, extracts and summaries of it, must be handled and stored securely, so as to minimise the risk of loss. It must be held so as to be inaccessible to persons who are not required to see the material (where applicable). This requirement applies to all those who are responsible for the handling of the material. It will be necessary to ensure that an appropriate security clearance regime is in place to safeguard the material whether held electronically or physically.

24.19 COPYING

24.20 Material obtained through covert surveillance may only be copied to the extent necessary for the authorised purposes set out above. Copies include not only direct copies of the whole of the material, but also extracts and summaries which identify themselves as the product of covert surveillance, and any record which refers to the covert surveillance and the identities of the persons to whom the material relates.

24.21 In the course of an investigation, the Council must not act on or further disseminate legally privileged items unless it has first informed the IPC that the items have been obtained.

24.22 DESTRUCTION

24.23 Information obtained through covert surveillance, and all copies, extracts and summaries which contain such material, should be scheduled for deletion or destruction and securely destroyed as soon as they are no longer needed for the authorised purpose(s) set out above. If such information is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid. In this context, destroying material means taking such steps as might be necessary to make access to the data impossible.

25. ERRORS

25.1 Proper application of the surveillance provisions in the RIPA codes and this Policy should reduce the scope for making errors.

25.2 RELEVANT ERROR

25.3 An error must be reported if it is a "**relevant error**". A relevant error is any error by the Council in complying with any requirements that are imposed on it by any enactment which are subject to review by a Judicial Commissioner. This would include compliance by public authorities with Part II of RIPA.

25.4 Examples of relevant errors occurring would include circumstances where:

- Surveillance activity has taken place without lawful authorisation.
- There has been a failure to adhere to the safeguards set out in the relevant statutory provisions and Chapter 9 of the Surveillance Codes of Practice relating to the safeguards of the material.

25.5 Errors can have very significant consequences on an affected individual's rights. All relevant errors made by the Council must be reported to the Investigatory Powers Commissioner as soon as reasonably practicable, and a full report no later than ten working days after the error is discovered. The report should include information on the cause of the error; the amount of surveillance conducted, and material obtained or disclosed; any unintended collateral intrusion; any analysis or action taken; whether any material has been retained or destroyed; and a summary of the steps taken to prevent recurrence.

25.6 SERIOUS ERRORS

25.7 The Investigatory Powers Commissioner must inform a person of any relevant error relating to that person if the Commissioner considers that the error is a **serious error** and that it is in the public interest for the person concerned to be informed of the error. The Commissioner may not decide that an error is a serious error unless they consider that the error has caused significant prejudice or harm to the person concerned. The fact that there has been a breach of a person's convention rights (within the meaning of the HRA) is not sufficient by itself for an error to be a serious error.

25.8 It is important that all staff involved in the RIPA process report any issues, so they can be assessed as to whether it constitutes an error which requires reporting.

26. COMPLAINTS

26.1 The Investigatory Powers Tribunal (IPT) has jurisdiction to investigate and determine complaints against the Council's use of investigatory powers, including those covered by this code. Any complaints about the use of powers as described in this code should be directed to the IPT.

26.2 Complaints should be addressed to:
The Investigatory Powers Tribunal
PO Box 33220
London
SWIH 9ZQ

Investigatory Powers Act 2016
Acquisition of Communications Data Policy

Appendix

Version Control:	
Document Name:	Investigatory Powers Act 2016 Acquisition of Communications Data Policy
Version:	1
Responsible Officer:	Emma Cathcart, Counter Fraud Unit
Approved by:	
Date First Approved:	
Next Review Date	
Retention Period:	N/A

Revision History

Revision date	Version	Description
April 2019	1	Change in legislation / introduction of IPA 2016

Consultees

Internal	External
Audit Committee	
Legal Department	
Corporate Management	

Distribution

Name	
Enforcement Officers	

CONTENTS

1. INTRODUCTION

1.1. The Investigatory Powers Act 2016 (IPA) governs how law enforcement agencies use the investigatory powers available to them, in relation to the lawful acquisition of Communications Data (CD). The IPA provides unprecedented transparency and substantial privacy protection, strengthening safeguards and introducing oversight arrangements. It also introduces a powerful new Investigatory Powers Commission (IPC) to oversee how these powers are used.

1.2. The powers provided by the Regulation of Investigatory Powers Act 2000 (RIPA) allowed the Council to obtain CD from Communications Service Providers (CSPs) in connection with criminal investigations.

1.3. The IPA extends the range of data Councils are able to request from providers but ensures independent authorisation for the acquisition through the new Office for Communications Data Authorisations (OCDA). However, it continues only to be a justifiable interference with an individual's human rights if such conduct is authorised, is both necessary and proportionate, and is in accordance with the law.

1.4. All applications for CD must be made via an Accredited Officer known as a Single Point of Contact (SPoC) who has passed a Home Office approved course. All Councils must use the National Anti-Fraud Network (NAFN) as their SPoC. Therefore, all applications to access CD will be made through NAFN via their online application service.

1.5. The introduction of OCDA means the acquisition of CD by Council officers no longer requires judicial approval.

1.6. These powers should not be confused with any Policy and practices with regard to monitoring under the lawful business practices legislation. This latter legislation relates to the monitoring of the Council's own communication and computer systems.

2. SCOPE OF POLICY

2.1. This Policy sets out the Council's procedures and approach for obtaining and handling CD for the purposes of preventing or detecting crime or of preventing disorder; the only lawful reasons for Council staff to use IPA legislation to access CD.

2.2. This Policy should be read in conjunction with the Communications Data Code of Practice (COP), currently in draft. This also creates a system of safeguards, consistent with the requirements of Article 8 (rights to privacy) of the Human Rights Act 1998. The Codes of Practice are admissible in evidence in criminal and civil proceedings.

2.3. The draft Code can be obtained using the link detailed below and is available to all Council staff involved in the acquisition of CD.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757851/Communications_Data_Code_of_Practice.pdf

2.4. Both this Policy and the COP will be followed at all times and under no circumstances should access to CD be sought outside of this guidance.

2.5. The Council will review and amend this Policy as necessary to ensure that it continues to remain compliant and meets legislative requirements and the objectives of the Council.

3. ROLES OF STAFF INVOLVED IN THE PROCESS

3.1. The process for the acquisition of CD under the IPA requires the following personnel:

- Applicant
- Designated Person (DP)
- Single Point of Contact (SPoC)
- OCDA Authorising Individual

4. APPLICANT

4.1. The Applicant is a person involved in conducting an investigation or operation who makes an application in writing for the acquisition of CD. The Applicant completes an application form, setting out for consideration the necessity and proportionality of a specific requirement for acquiring CD. Prior to the completion of the relevant paperwork, it may be advisable for the Applicant to consult with the SPoC at NAFN.

5. DESIGNATED PERSON

5.1. The DP is a person of Service Manager level or equivalent within the Council who confirms to NAFN that they are aware that an application has been made. They do not have any authorising function but are responsible for the integrity of the process in place and the overall quality of that process.

6. SINGLE POINT OF CONTACT

6.1. The SPoC is either an accredited individual (passed the Home Office course) or a group of accredited individuals such as the National Anti-Fraud Network, who are trained to facilitate lawful acquisition of CD. All accredited officers are issued a Personal Identification Number (PIN). Details of all accredited individuals are available to Communication Service Providers (CSPs) for authentication purposes.

6.2. An accredited SPoC promotes efficiency and good practice in ensuring only practical and lawful requirements for CD are undertaken. The SPoC provides objective judgement and advice to the Applicant and provides a "guardian and gatekeeper" function, ensuring that public authorities act in an informed and lawful manner.

6.3. As already explained, this Council can only use the services of NAFN as the Council's SPoC. Therefore, all applications to access CD will be made through NAFN.

6.4. The SPoC will be in a position to:

- Engage proactively with Applicants to develop strategies to obtain CD and use it effectively in support of operations or investigations;
- Assess whether the acquisition of specific CD from a CSP is reasonably practical or whether the specific data required is inextricably linked to other data;
- Advise Applicants on the most appropriate method for the acquisition of data where the data sought engages a number of CSPs;
- Advise Applicants on the type of data that can be obtained to meet their purposes.
- Provide assurance to DPs that Authorisations and Notices are lawful under the IPA and free from errors;
- Provide assurance to OCDA that an application has been verified and checked.

- Assess whether CD disclosed by a CSP in response to a Notice fulfils the requirement of the Notice;
- Assess whether CD obtained by means of an Authorisation fulfils the requirement of the Authorisation;
- Assess any cost and resource implications to both the Council and the CSP of data requirements.

7. OCDA AUTHORISING INDIVIDUAL

7.1. The OCDA officer receives the application from the NAFN SPoC and checks the application meets the necessary criteria before authorising or rejecting and issuing a Decision Document. NAFN will retain the original of all the documents. These will be retained within the on-line portal. Copies of the documents must be retained by the Applicant, DP or within the relevant department for inspection by the IPC and for audit, filing and disclosure purposes under the Criminal Procedures Investigation Act 1996. (OCDA will only hold the applications and Decision Documents for a limited period of time due to the degree of sensitivity and risk arising from the accumulation of these documents in a central database.)

8. WHAT IS COMMUNICATIONS DATA

8.1. CD does not include the content of any communication. It is not lawfully possible for Council employees under any circumstances to obtain the content of communications.

8.2. The term 'CD' embraces the 'who', 'when' and 'where' of a communication but not the content - not what was said or written. It includes the manner in which, and by what method, a person or machine communicates with another person or machine. It excludes what they say or what data they pass on within a communication including text, audio and video

8.3. CD can include the address to which a letter is sent, the time and duration of a communication, the telephone number or email address of the originator and recipient, and the location of the device from which the communication was made. It covers electronic communications including internet access, internet telephony, instant messaging and the use of applications. It also includes postal services.

8.4. CD is generated, held or obtained in the provision, delivery and maintenance of communications services – i.e. postal services or telecommunications services.

8.5. Where the provision of a communication service engages a number of providers, the SPoC will determine the most appropriate plan for acquiring the data.

8.6. When enquiries regarding CD are being considered within an investigation, it may be advisable that Applicants seek advice and guidance from the SPoC at NAFN. The RIPA Coordinator /DP within the Counter Fraud Unit can provide contact details.

9. COMMUNICATIONS DATA DEFINITIONS

9.1. The IPA introduces new terminology for CD – Entity Data and Events Data

9.2. Entity Data describes the 'who' involved in the communication – the subscriber and the links between different entities or communicators. Entities could be individuals, groups and objects (such as mobile phones or other communications devices).

9.3. Examples of entity data requests include:

- Subscriber checks, such as who is the subscriber of phone number 01234 567 890?
- Who is the account holder of e-mail account example@example.co.uk?
- Who is entitled to post to web space www.example.co.uk?
- Subscribers' or account holders' account information, including names and addresses for installation, and billing including payment method(s), details of payments e.g. for pre-paid mobiles.
- Information about the connection, disconnection and reconnection of services to which the subscriber or account holder is allocated or has subscribed (or may have subscribed) including conference calling, call messaging, call waiting and call barring telecommunications services.
- Information about apparatus or devices used by, or made available to, the subscriber or account holder, including the manufacturer, model, serial numbers and apparatus codes.
- Information about selection of preferential numbers or discount calls.

9.4. Event Data identifies or describes events in relation to a telecommunications system which consists of one or more entities engaging in an activity at a specific point or points in time – the 'what, when and where'. For obtaining Event Data there is a Serious Crime Threshold (see 19.1)

9.5. Examples of events data include, but are not limited to:

- Information tracing the origin or destination of a communication that is, or has been, in transmission (including incoming call records);
- Information identifying the location of apparatus when a communication is, has been or may be made or received (such as the location of a mobile phone);
- Information identifying the sender or recipient (including copy recipients) of a communication from data comprised in or attached to the communication;
- Routing information identifying apparatus through which a communication is or has been transmitted (for example, file transfer logs and e-mail headers – to the extent that content of a communication, such as the subject line of an e-mail, is not disclosed);
- Itemised telephone call records (numbers called)12;
- Itemised internet connection records;
- Itemised timing and duration of service usage (calls and/or connections);
- Information about amounts of data downloaded and/or uploaded;
- Information about the use made of services which the user is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services.

10. POSTAL DEFINITIONS

10.1. A postal service is a service which involves one or more of the collection, sorting, conveyance, distribution and delivery of postal items and where its main purpose is to

make available or facilitate the transmission of postal items containing communications. CD in relation to a postal service is defined at section 262(3) of the IPA and comprises three elements:

- Postal data which is or has been comprised in or attached to a communication for the purpose of the service by which it is transmitted;
- Data relating to use made by a person of a postal service;
- Information held or obtained by a postal operator about persons to whom the postal operator provides or has provided a communications service and which relates to the provision of the service.

10.2. Postal data is defined in section 262(4) of the IPA and includes specified categories of data written on the outside of a postal item. All information on the outside of a postal item concerning its postal routing, for example the address of the recipient, the sender and the post-mark, is postal data.

10.3. In the postal context anything included inside a postal, item, which is in transmission, will be content. Any message written on the outside of a postal item which is in transmission may be content and fall within the scope for the interception of communications. For example, a message written by the sender for the recipient will be content but a message written by a postal worker concerning the delivery of the postal item will not. All information on the outside of a postal item concerning it's routing, for example the address of the recipient, the sender and the postmark, is postal data and will not be content.

11. WEB BROWSING AND COMMUNICATIONS DATA

11.1. Web browser software provides one way for users to access web content. When using a browser to access the web, a user may enter a web address. These are also referred to as uniform resource locators (URLs). In order to access a webpage over the internet, key parts of a URL are normally converted from a web address format to a numeric IP address which assists in identifying the host. Some elements of a URL are necessary to route a communication to the intended recipient and are therefore CD.

11.2. The URL may also contain the port, which is an extended part of the Internet Provider (IP) address and the user information – including usernames and authorisations. When required to route a communication, the port and user information will be CD.

12. RELEVANT COMMUNICATIONS DATA

12.1. A data retention notice under the IPA may only require the retention of relevant CD. This is defined at section 87 of the IPAt and is a subset of CD.

It is data which may be used to identify or assist in identifying any of the following:

- The sender or recipient of a communication;
- The time or duration of a communication;
- The type, method or pattern, or fact of a communication;
- The telecommunication system to or through which a communication is transmitted;
- The location of any such system.

13. INTERNET CONNECTION RECORDS

13.1. An internet connection record (ICR) is a record of an event held by a telecommunications operator about the service to which a customer has connected on the internet. An ICR is CD.

13.2. An ICR will only identify the service that a customer has been using. For example many social networking apps on a device maintain persistent connections to a service. Even in this case the relevant ICR will signpost the service accessed by the device, enabling the authority to make further enquiries of the social networking provider identified.

13.3. Further detail on the definitions described above and the types of CD that can be accessed is available in the COP.

13.4. The SPoC will provide advice and assistance with regard to the types of data which can be lawfully obtained and how that data may assist an investigation. Where an applicant is unsure of the category of data they are seeking (entity or events data) or what additional types of CD may be retained by a telecommunications operator or postal operator for their own business use, the applicant should discuss this with their Single Point of Contact (SPoC).

14. PREPAID MOBILE PHONES

14.1. Unregistered prepaid mobile phones are common amongst criminals as it allows them to avoid detection more easily. It is possible that a subscriber check will identify a number as belonging to one of these devices. This does not necessarily prevent an investigating officer obtaining useful information. The Applicant can ask for further information about the subscriber under section 21(4)(c), including top-up details, method of payment, the bank account used or customer notes etc.

14.2. So as to allow for the widening of the data capture, the Applicant should outline in their original application that further information will be required if the phone turns out to be prepaid, this information could be requested in two stages. Firstly, asking for the subscriber details and then, if this turns out to be an unregistered prepaid phone, asking for the further information.

14.3. The information that is received can then be developed to try to obtain further information about the user of the phone. Solution Providers such as EasyPay, EPay etc. are the third parties involved in the transaction of credit placed on a mobile phone. If a Solution Provider is provided with the mobile telephone number, the transaction date and the transaction number, they are often able to provide the method of payment and the location of the top-up. Solution Providers are not CSPs and therefore they cannot be issued with a Notice under the IPA; instead the data can be applied for under the Data Protection Act via the SPoC.

15. WHO CAN COMMUNICATIONS DATA BE OBTAINED FROM?

15.1. CD can be obtained from a Communications Service Provider (CSP). A CSP is an operator who provides a postal service such as Royal Mail or telecommunications service, such as the usual telephone service providers. However, there may be less obvious companies which may be classed as a CSP. The SPoC at NAFN will determine which CSP they will contact to obtain the data on behalf of the Applicant. However, any intelligence obtained which establishes which CSP may provide the data should be included within the application or by notifying the SPoC.

16. LAWFUL REASONS TO ACCESS COMMUNICATIONS DATA

16.1. As mentioned earlier the Council's only lawful reasons to access CD is for the purpose of preventing or detecting crime or of preventing disorder.

16.2. Detecting crime includes establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed, the gathering of evidence for use in any legal proceedings and the apprehension of the person (or persons) by whom any crime was committed.

16.3. The Council can only lawfully process and consider applications to access CD on behalf of the Council. Under no circumstances will applications be accepted for outside authorities/agencies. However, it may be necessary during joint investigations to obtain CD; in these circumstances the Council can only apply for data which it would usually be allowed to access. It should be clear in the investigation Policy log that it is a joint investigation as it may have to be justified to a Court or Tribunal.

16.4. Staff must not apply on behalf of any third parties who do not have lawful authority to obtain CD. Should an organisation make such an approach this must be reported to the Senior Responsible Officer (SRO) who has the responsibility for the Council's working practices in relation to obtaining CD.

16.5. Where the Council is contracted to undertake work on behalf of a third party, CD may be obtained if the Council is the investigating and prosecuting body.

17. USING OTHER POWERS

17.1. The IPA is the primary legislation for the acquisition of CD and should always be the first option considered due to the rigorous and independent assessment and authorisation process.

18. INTERNAL INVESTIGATIONS

18.1. The Codes state 'where an investigation relates to an allegation of criminal conduct by a member of a public authority, that public authority (or another public authority appointed to investigate the complaint) may use their powers under Chapter II to obtain CD for the purpose of preventing and detecting the alleged or suspected crime where the investigating officer intends the matter to be subject of a prosecution within a criminal court. Should it be determined there are insufficient grounds to continue the investigation or insufficient evidence to initiate a prosecution within a criminal court, it will, with immediate effect, no longer be appropriate to obtain CD under the Act'.

18.2. If CD is sought in connection with officers of the Council committing crimes against the Council, it is important that the enquiry is a genuine criminal investigation with a view to proceeding criminally as opposed to just a disciplinary matter. Advice may be required from the Council's Legal section if this arises.

19. SERIOUS CRIME THRESHOLD

19.1. With effect from 1st November 2018 the IPA introduced a new Serious Crime Threshold to applications for CD. This means the Council may only acquire Events Data where the crime can be defined as a serious crime. Where the crime cannot be defined as serious, only Entity Data may be obtained.

19.2. The following definitions of serious crime apply:

- An offence that is capable of attracting a prison sentence of 12 months or more;
- An offence by a person who is not an individual (i.e. a corporate body);
- An offence falling within the definition of serious crime in section 263(1)of the IPA (i.e. where the conduct involves the use of violence, results in substantial financial gain or is by a large number of persons in pursuit of a common purpose);
- An offence which involves, as an integral part of it, the sending of a communication;
- An offence which involves, as an integral part of it a breach of a person's privacy.

20. NECESSITY AND PROPORTIONALITY

20.1. The COP states the acquisition of CD under the IPA will be a justifiable interference with an individual's human rights under Article 8 Right to Privacy, only if the conduct being authorised or required to take place is both necessary and proportionate and in accordance with law.

20.2. Below is guidance to assist Applicants with factors that impact on necessity and proportionality.

21. NECESSITY

21.1. In order to justify the application is necessary, the Applicant needs as a minimum to consider three main points:

1. The event under investigation, such as a crime or disorder offence;
2. The person, such as a suspect, witness or missing person and how they are linked to the event;
3. The Communication Data, such as a telephone number or IP address, and how this data is related to the person and the event.

21.2. In essence, necessity should be a short explanation of 1**) the event**, 2**) the person and 3) the CD and how these three link together.** The application must establish a link between the three aspects to be able to demonstrate the acquisition of CD is necessary for the statutory purpose specified.

21.3. Necessity does not entail explaining 'what will be achieved by acquiring the data' or 'why specific time periods have been requested', these points are relevant to proportionality and should be covered in the relevant section to stop repetition.

22. PROPORTIONALITY

22.1. Applicants should include an outline of how obtaining the data will benefit the investigation or operation. If more than one item of data is being sought, the relevance of the additional data should be explained.

22.2. This outline should include an explanation of how the level of intrusion is justified when taking into consideration the benefit the data will give to the investigation. This justification should include confirmation that relevant less intrusive investigations have already been undertaken where possible. For example, the subscriber details of a phone number may be obtained from online enquiries or other publicly available sources.

22.3. The relevance of any time periods requested must be explained, outlining how these periods are proportionate to the event under investigation. The two basic questions are:

- What are you looking for in the data to be acquired and;
- If the data contains what you are looking for, what will be your next course of action?

22.4. Particular consideration should be given to any periods of days or shorter periods of time which might achieve the objective. They should specify the shortest period in which the objective for which the data is sought can be achieved. To do otherwise will impact on the proportionality of the Authorisation or Notice and impose unnecessary burden upon a CSP.

22.5. An explanation as to how CD once acquired will be used, and how it will benefit the investigation or operation will enable the Applicant to set out the basis of proportionality.

22.6. An explanation of the proportionality of the application should include a consideration of the rights (particularly to privacy and, in relevant cases, freedom of expression) of the individual and a balancing of these rights against the benefit to the investigation.

22.7. An examination of the proportionality of the application should also involve consideration of possible unintended consequences and, when relevant this should be noted. Unintended consequences of an application are outcomes that are not intended by the application.

23. COLLATERAL INTRUSION

23.1 Consideration of collateral intrusion forms part of the proportionality considerations and becomes increasingly relevant when applying for Events Data. Applications should include details of what collateral intrusion may occur and how the time periods requested impact on the collateral intrusion.

23.2 The question to be asked is 'Will the data set to be acquired result in collateral intrusion to persons outside the line of enquiry the data is being obtained for?' For example, itemised billing on the subject's family home will be likely to contain calls made by the family members.

23.3 Applicants should not write about a potential or hypothetical 'error' and if the Applicant cannot identify any meaningful collateral intrusion, that factor should be recorded in the application i.e. 'none identified'.

23.4 It is accepted that for a straight forward subscriber check there will be no meaningful collateral intrusion.

24. THE TWO WAYS OF OBTAINING COMMUNICATIONS DATA

24.1. The legislation provides two different methods of acquiring CD (see below). The SPoC at NAFN will be responsible for deciding the process for obtaining the data required and passing responses from the service provider to the Council.

24.2. The two methods are:

- **Authorisation of conduct,** or
- **Authorisation to give a Notice**

24.3. An authorisation of conduct to acquire CD may be appropriate where, for example:

- there is an agreement in place between a public authority and a telecommunications operator or postal operator to facilitate the secure and swift disclosure of CD. Many telecommunications operators and postal operators have auditable acquisition systems in place to ensure accurate and timely acquisition of CD, while maintaining security and an audit trail;
- where the data can be acquired directly from a telecommunication system and the activity does not constitute interception or equipment interference; or
- a public authority considers there is a requirement to identify a person to whom a service is provided but the specific telecommunications operator or postal operator has yet to be conclusively determined as the holder of the CD.

An authorisation to give a notice may be appropriate where a telecommunications operator or postal operator is known to be capable of disclosing (and, where necessary, obtaining) the CD

25. THE APPLICATION PROCESS

25.1. From April 2019 the IPA removes the requirement to obtain judicial approval. Applications will only require Independent Authorisation.

25.2. Prior to an Applicant applying for CD, they should contact a SPoC at NAFN who will be in a position to advise them regarding the obtaining and use of CD within their investigation. This will reduce the risk of the Applicant applying for data which they are not able to obtain. It will also assist the Applicant to determine their objectives and apply for the most suitable data for those circumstances.

25.3. The Council will use the automated application process provided by NAFN. This automated service contains the relevant documentation for the Applicant to complete the relevant forms.

25.4. To use the system, Applicants and the DP have to individually register on the NAFN website - www.nafn.gov.uk. A number of departments within the Council have contributed towards the NAFN annual membership fee; therefore an Applicant needs to confirm with their Line Manager that they are allowed to register. Should you have any queries, please contact the Counter Fraud Unit.

25.5. With regard to shared services, the Council on whose behalf the request is being made must be a member of NAFN and the request made via login details for that Council. Applicants and DPs cannot make use of one Council's membership to obtain any information on behalf of another. Login details will be necessary for each Council that an individual is employed by or works on behalf of.

25.6. The online application form, once completed by the Applicant will be forwarded electronically to a SPoC at NAFN who will then perform their responsibilities and if required they will contact the Applicant regarding the contents of the application form. The SPoC at NAFN will obtain confirmation from the nominated DP that they are aware of the application before proceeding.

25.7. The SPoC confirms that the Council is permitted to use the recorded statutory purpose and determines the conduct to satisfy the Council's need (the type of data that is required). If event data is required the SPoC checks the Applicant has recorded a description of the offence(s) and a justification for the seriousness of the offence(s)

25.8. The SPoC can return the application to the Council for a re-work if it does not meet the necessary criteria.

25.9. Once approved the SPoC refers the application to OCDA for authorisation. OCDA then return the application to NAFN for the SPoC to obtain the authorised data from the CSP.

25.10. If the OCDA officer rejects the application it can be returned to the applicant for a re-work.

26. TIME SCALES

26.1. A new Operational Prioritisation has been introduced to enable NAFN to convey to OCDA the operational urgency for the acquisition of data and ensure it is appropriately triaged and handled to meet these demands.

26.2. Operational Prioritisation is categorised in Priority Levels 1-4 and for each Priority rating there is an expected Service response time.

26.3. The Council will generally be submitting requests that are Priority Level 4 – Routine- for which the response should be within 4 working days or 60 working hours.

27. APPLICATION FORM

27.1. The Applicant will complete an application form setting out for consideration the necessity and proportionality of a specific requirement for CD.
An application to acquire CD must:

- describe the CD required, specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s);
- specify the purpose for which the data is required, by reference to a statutory purpose under the Act;
- include a unique reference number;
- include the name and the office, rank or position held by the person making the application;
- describe whether the CD relates to a victim, a witness, a complainant, a suspect, next of kin, vulnerable person or other person relevant to the investigation or operation;
- identify and explain the time scale within which the data is required;
- explain why the acquisition of that data is considered necessary and proportionate to what is sought to be achieved by acquiring it;
- present the case for the authorisation in a fair and balanced way. In particular, all reasonable efforts should be made to take account of information which supports or weakens the case for the authorisation;

- consider and, where appropriate, describe any meaningful collateral intrusion – the extent to which the rights of any individual not under investigation may be infringed and why that intrusion is justified in the circumstances;
- consider and, where appropriate, describe any possible unintended consequences of the application; and
- where data is being sought from a telecommunications operator or postal operator, specify whether the telecommunications operator or postal operator may inform the subject(s) of the fact that an application has been made for their data
- include the operation name (if applicable) to which the application relates;

28. URGENT ORAL AUTHORISATION

28.1. There is no provision within the legislation for the Council to orally provide authority to obtain CD. All requests will be made in writing on the NAFN portal and require authorisation from a DP.

29. ERRORS

29.1. There is a requirement to record or in some instances report to IPCO errors that occur when accessing CD. The thorough checking of operating procedures, including the careful preparation and checking of applications, Notices and Authorisations, should reduce the scope for making errors. Attention to detail will be required by all persons involved in the process.

29.2. Reporting and recording of errors will draw attention to those aspects of the process of acquisition and disclosure of CD that require further improvement to eliminate errors and the risk of undue interference with any individual's rights. Therefore, the SPoC or other persons involved in the process should bring to the immediate attention of the SRO either a recordable error or a reportable error and the necessary action can then be taken in line with the COP.

29.3. Where material is disclosed by a CSP in error, which has no connection or relevance to any investigation or operation undertaken by the public authority receiving it, that material and any copy of it should be destroyed as soon as the report to the Commissioner has been made.

29.4. An error can only occur after:

- The granting of an Authorisation and the acquisition of data has been initiated, or
- Notice has been given and the Notice has been served on a CSP in writing, electronically or orally.

29.5. It is important to apply the procedures correctly to reduce the risk of an error occurring. Where any error occurs, a record will be kept.

29.6. There are two types of errors:

- Reportable
- Recordable

30. REPORTABLE ERROR

30.1. Where CD is acquired or disclosed wrongly a report must be made to the IPCO. Such errors can have very significant consequences on an affected individual's rights with details of their private communications being disclosed to a public authority and, in extreme circumstances, being wrongly detained or wrongly accused of a crime as a result of that error.

30.2. Examples can include:

- An Authorisation or Notice made for a purpose, or for a type of data which the relevant public authority cannot call upon or seek, under the Act;
- Human error, such as incorrect transposition of information from an application to an Authorisation or Notice;
- Disclosure of the wrong data by a CSP when complying with a Notice;
- Acquisition of the wrong data by a public authority when engaging in conduct specified in an Authorisation;

30.3. Any reportable error must be reported to the SRO as soon as it is identified and then a report will be made to the IPCO within five working days. The report must contain the unique reference number of the Notice and details of the error, plus an explanation how the error occurred and indicate whether any unintended collateral intrusion has taken place. It will also provide an indication of the steps that will take place to prevent a reoccurrence. The 'reporting an error by accredited SPoC form' (CD5) should be used for this purpose.

30.4. If the report relates to an error made by a CSP, the Authority must still report it. The CSP should also be notified to enable them to investigate the cause.

31. RECORDABLE ERROR

31.1. In cases where an error has occurred but is identified by the public authority or the CSP without data being acquired or disclosed wrongly, a record will be maintained by the Council and NAFN of such occurrences. These records must be available for inspection by the IPCO.

31.2. The staff involved in the process of acquiring CD must report errors once they have been identified. It will not be acceptable for the error to be ignored.

31.3. Examples can include:

- A Notice given, which is impossible for a CSP to comply with and an attempt to impose the requirement has been undertaken by the public authority;
- Failure to review information already held, for example unnecessarily seeking the acquisition or disclosure of data already acquired or obtained for the same investigation or operation, or data for which the requirement to acquire or obtain it is known to be no longer valid.

32. EXCESS DATA

32.1. Where authorised conduct results in the acquisition of excess data, the excess data acquired or disclosed should only be retained by the public authority where appropriate to do so – for example in relation to a criminal investigation.

32.2. Where a public authority is bound by the Criminal Procedure and Investigations Act 1996 and the IPA Codes of Practice, there will be a requirement to record and retain

data which is relevant to a criminal investigation, even if that data was disclosed or acquired beyond the scope of a valid authorisation.

32.3. If having reviewed the excess data, it is intended to make use of the excess data in the course of the investigation or operation, an applicant must set out the reason(s) for needing to use that material in an addendum to the application upon which the authorisation or notice was originally granted or given. The SRO (or a person of equivalent grade or authority) will review the data and consider whether it is necessary and proportionate for the excess data to be used in the investigation.

32.4. As with all CD, the requirements of relevant data protection legislation and data retention policies should be adhered to in relation to excess data.

33. RECORD KEEPING AND SECURITY OF DATA

33.1. All the records and any data obtained must be kept secure and confidential.

33.2. The Council must retain copies of all Applications, as a printed copy of the online application submitted via NAFN, and any other associated documentation where copies have been provided by the NAFN SPoC. This will be coordinated by the RIPA Coordinating Officer/DP who also holds copies of applications for surveillance as per the Council's overarching RIPA Policy.

33.3. The copy application records must be available for inspection by the IPCO. The IPCO will also be able to obtain copies direct from NAFN.

33.4. The SRO will have access to all of these forms as and when required.

33.5. The Council must also keep a record of the following:

- Number of applications submitted to the NAFN SPoC;
- Number of applications submitted to the NAFN SPoC which were referred back to the Applicant for amendment or declined by the SPoC;
- The reason for any amendments being required or application being declined by the SPoC;
- The reason for any referrals back or rejections;
- Whether any part of the application relates to a person who is member of a profession that handles privileged or otherwise confidential information (such as a Medical Doctor, Lawyer, Journalist, MP or Minister of Religion (and if so, which profession);

34. CRIMINAL PROCEDURES AND INVESTIGATIONS ACT 1996 (CPIA)

34.1. The Criminal Procedure and Investigations Act 1996 (CPIA) requires that material which is obtained in the course of an investigation and which may be relevant to the investigation must be recorded, retained and revealed to the prosecutor. Therefore, all material relating to the accessing of CD falls under these provisions. If the Applicant is not the Disclosure Officer in the case, they must make the Disclosure Officer aware of all of the material relating to the application and acquisition of the CD.

34.2. All material which may be relevant to the investigation must be retained until a decision is taken whether to institute proceedings against a person for an offence and if prosecuted, at least until the accused is acquitted or convicted, or the prosecutor decides not to proceed with the case and in line with the Council's Data Retention Policies.

34.3. Where the accused is convicted, the data which is relevant must be retained at least for six months from the date of conviction, and where the court imposes a custodial sentence, until the convicted person is released from custody.

34.4. If the court imposes a custodial sentence and the convicted person is released from custody earlier than six months from the date of conviction, all material which may be relevant must be retained at least until six months from the date of conviction and in line with the Council's Data Retention Policies.

35. DATA PROTECTION ACT 2018 (DPA) AND THE GENERAL DATA PROTECTION REGULATIONS (GDPR)

35.1. CD acquired or obtained under the provisions of the IPA, and all copies, extracts and summaries of it must be handled and stored securely in line with the requirements of data protection legislation and regulations.

35.2. There is no provision in the IPA preventing CSPs from informing individuals about the disclosure of their CD in response to a Subject Access Request. However, a CSP may exercise certain exemptions to the right of subject access. If a CSP receives a Subject Access Request they must carefully consider whether in the particular case, disclosure of the fact of the Notice would be likely to prejudice the prevention or detection of crime.

35.3. Should a request for advice be made from a CSP to the SPoC regarding a disclosure, the SPoC will consult with the Data Protection Officer for the Council and the Applicant if necessary before a decision is made. Each case should be examined on its own merits.

35.4. Equally, these rules will apply should a Subject Access Request be made from an individual where material under this legislation is held by the Council.

35.5. A record will be made of the steps taken in determining whether disclosure of the material would prejudice the apprehension or detection of offenders. This might be useful in the event of the data controller having to respond to enquiries made subsequently by the Information Commissioner and the courts etc.

36. OVERSIGHT

36.1. The IPA provides for an Investigatory Powers Commissioner (IPC) whose remit includes providing comprehensive oversight of the use of the powers contained within the IPA and adherence to the practices and processes in the Code of Practice. They carry out inspections, and for the purposes of Council applications, carry out inspections of NAFN. Should they have any concerns regarding an application they would contact the relevant staff involved at the Council. It is possible that they could also inspect the Council.

36.2. It is important to note that should the Commissioner establish that an individual has been adversely affected by any wilful or reckless failure by any person within a relevant public authority exercising or complying with the powers and duties under the IPA in relation to the acquisition or disclosure of CD, he shall, subject to safeguarding national security, inform the affected individual of the existence of the Tribunal and its role. The Commissioner should disclose sufficient information to the affected individual to enable him or her to effectively engage the Tribunal.

37. COMPLAINTS

37.1. The Information Commissioner is responsible for the oversight of the security, integrity and destruction of data retained in accordance with the Act. Any concerns about compliance with data protection and related legislation should be passed to the ICO at the following address:

37.2.

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
0303 123 1113
www.ico.org.uk

The Investigatory Powers Tribunal (IPT) has jurisdiction to consider and determine complaints regarding public authority use of investigatory powers, including those covered by the IPA.

The IPT is an independent body made up of members of the judiciary and senior members of the legal profession. Following receipt of a complaint the IPT can undertake its own enquiries and complaints and can demand access to all information necessary. Information regarding the IPT and how to make a complaint can be found at www.ipt-uk.com, or by writing to:

The Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ

38. STRATEGY AND POLICY REVIEW

38.1. The Counter Fraud Unit 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.

Responsible Department: Counter Fraud Unit

Date: April 2019

Review frequency as required by legislative changes / every year.

This page is intentionally left blank