STROUD DISTRICT COUNCIL
www.stroud.gov.uk

Information Governance Policy Framework

January 2021

Corporate Policy & Governance

Last updated: 21/04/21

Next document review by:

Reviewed by: *Name, Service, Team*

Approved by: *Name or Committee*

Amendment History

New Version Number	Issued By	Nature of amendment	Approved by & Date	Date on Intranet
0.1	Information Governance Officer	First Draft for comments	Pat Arran 21/04/2021	21/04/2021

1. Scope

This policy extends to all employees, contractors, agents, consultants, partners or other persons engaged in the council's service delivery, together with and elected members (in terms of information received, created or held by an elected member on behalf of the council)

2. Purpose

2.1 The purpose of the Information Governance Framework is to set out the council's responsibilities and activities in relation to information governance in accordance with current legislation and professional principles.

2.2 Information governance describes the approach within which accountability, standards, policies and procedures are developed and implemented, to ensure that all information created, obtained or received by the council is held and used appropriately.

2.3 This policy will provide a consistent approach and summarises the relevant regulations and commits the council to their application where appropriate.

3. Introduction

3.1 The council generates and receives a huge amount of data. It therefore acknowledges that information is one of its key assets and as such requires the same discipline to its management that it would to other important assets such as people, buildings and finances. Information assets can be both electronic or paper and include records and data sets held in back-office systems, network/shared drives, and within email systems.

3.2 It is vital that the council applies a robust management system in ensuring the efficient and effective operation of services, meeting security and regulatory requirements, and demonstrating accountability for decisions and activities taken.

3.3 Councils must have in place an effective framework in place for how they collect, process, access, store, share and delete information and it is important to have a consistent approach. This framework policy sets out best practices and standards which must be maintained together with responsibilities of individuals' for managing the information assets.

4. Aims & Objectives

4.1 The aim of Information Governance is to achieve excellence in the management of Information assets and records so that the council can:

- Comply with regulatory, legal, audit and discovery requests, ensuring that there is clear guidance for all staff.
- Access the right information from wherever it is needed, with permissions granted to the appropriate staff.
- Share business information both inside and outside the organisation where appropriate, using sharing agreements. Data sharing will be undertaken in accordance with the Information Commissioner's Data Sharing Code of Practice
- Manage records using good practice standards, including identifying vital records and their systems and ensuring that they are protected. Ensure that at least annually, the record of Processing Activities questionnaire is completed by all Service areas and the Record of Processing register is updated to reflect any changes.
- Control the unnecessary proliferation of information and remove duplicate or useless information, by encouraging staff to work closely together and enabling better use of resources and reducing the number of opportunities for data to be compromised.
- Dispose of information as soon as it reaches its legal and business usefulness in line with published Retention Policies
- Build an information governance culture where information and records are managed coherently and consistently across the council. Classify information under the correct record code by ensuring that staff follow the Records Management Policy.
- Align all line of business systems with Information Governance standards
- Educate employees about their Information Governance roles and responsibilities, by implementing a robust training plan, which sets out competencies for staff and the various ways to access learning.
- Be open and transparent by keeping publications scheme up-to-date and responding to requests for information as mandated by the government.

Documented procedures for Freedom of Information Requests and Environmental Information Requests are also available to the public on the council's website. Data Protection and FOI

- Ensure that we understand our own performance in relation to Information Governance and mange improvements in a systematic and effective way, working with Audit Risk Assurance to achieve an excellent standard of compliance.

5. Regulatory Environment

5.1 Stroud District Council recognises the need to fully comply with the requirements and obligations of the:

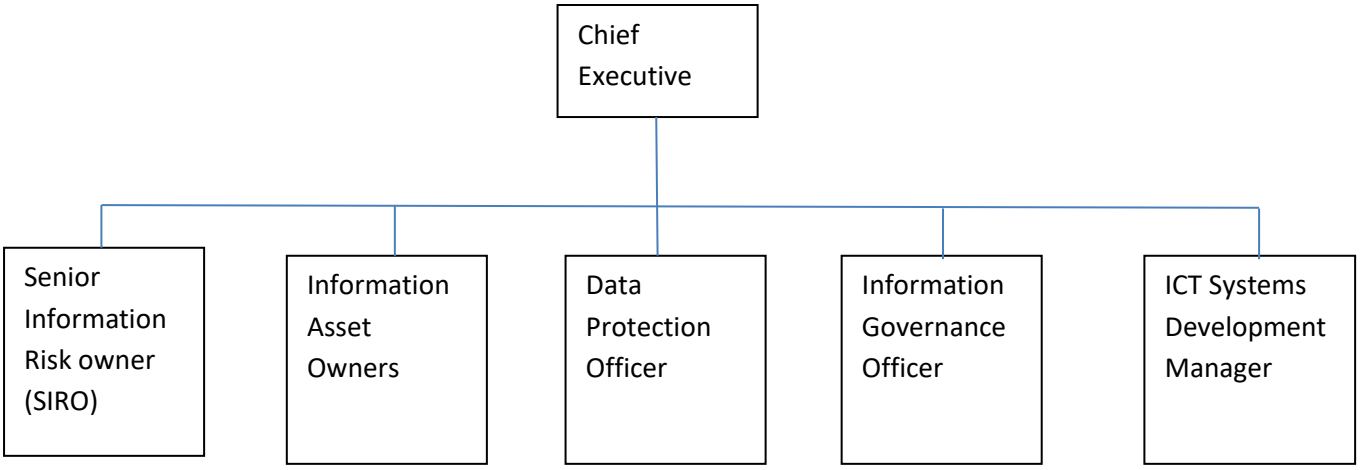
- General Data Protection Regulation (GDPR) 2018 – Regulates the processing of personal data and sets out the rights of data subjects
- Data Protection Act (DPA) 2018 – Clarifies some parts of the GDPR in the UK.
- Common law duty of confidentiality - Common law is not written out in one document like an Act of Parliament. It is a form of law based on previous court cases decided by judges; hence, it is also referred to as case law. The law is applied by reference to those

previous cases, so common law is also said to be based on precedent. The general position is that, if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the data subject's consent.

- Freedom of Information Act (FOIA) 2000 - Provides a right of access to the recorded information held by public bodies.
- Freedom of Information & Data Protection (Appropriate limits and fees) Regulations 2004 - Sets the Appropriate Limit and the Fees chargeable for FOIA and DPA.
- Environmental information Regulations (EIR) 2004 - Provides a right of access to the environmental information held by public bodies.
- Regulation of Investigatory Powers Act (RIPA) 2000 – This governs the use of covert surveillance by public bodies. This includes bugs, video surveillance and interceptions of private communications (e.g. phone calls and emails), and even undercover agents ('covert human intelligence sources').
- Human Rights Act 1998 – Article 8 provides rights in relation to privacy.

6. Information Governance Management

6.1 The council has an information governance agenda, which is led by an action plan built up from reviewing and monitoring the policies and processes on a regular basis. There are several key governance bodies identified within the framework, which meet to review and monitor action plans. The diagram below identifies the roles in our Information Governance Structure which are explained in more detail in Section 20 (Roles and Responsibilities).



6.2 The following policies and procedures, form part of the Information Governance framework and individually provide further details on the specific areas.

- Data Protection Policy
- Data Breach Policy
- Information Security
- Records Management Policy
- Information Complaints Policy
- Publications Scheme
- Anonymisation & Pseudonymisation Policy

6.3 Information as a corporate asset

- The council will create and maintain an inventory of its information assets.
- Information is made available unless there is a compelling reason not to, recognising all the relevant legislative and regulatory requirements. This applies to both internal and external users of information. Efforts are made to present and organise information to maximise its availability.
- The storage and organisation of information will promote its sharing, thereby minimising duplication of effort and the cost of its retrieval.
- All information will have a defined owner(s). It will be their responsibility to manage, protect and to make it available to others where required.
- The protection of information assets is carried out in accordance with council's Information Security Policy
- The management and retention of information will take into account its value to the council. Information will only be as retained as long as there is a business need and to ensure compliance with the relevant legal and regulatory requirements in line with the council's Records Management Policy.
- Disposal of information of a personal or confidential nature will be carried out securely and when there is no longer a legal or business need to keep it.
- Information ownership rights will be observed in that Information from third party sources will only be used in accordance with the licence or permissions granted.

7. Records Management

7.1 Good records management supports good data governance and data protection. Wider benefits include supporting information access, making sure that you can find information about past activities, and enabling the more effective use of resources.

7.2 The council recognises that its records are an important asset and are available to those who are entitled to see them. They are a key resource for the effective operation and accountability of the council. As with other assets, they require careful management and the Records Management Policy set out the council's responsibilities and activities to do this.

8. Compliance with the General Data Protection Regulation (GDPR) & Confidentiality Requirements

8.1 Compliance with GDPR

8.1.1 The council is fully committed to compliance with the requirements of the General Data Protection Regulation (GDPR). A Data Protection policy Data Protection Policy and well-designed procedures have been developed by the Corporate Policy & Governance Team, to ensure that all employees, elected members, contractors, partners or any other persons engaged with the council, who have access to any personal information held by or on behalf of the council, abide by their duties and responsibilities under the regulation.

8.1.2 The Data Protection Policy applies to all personal information held by the council or held on behalf of the council. This includes information held on paper and in electronic formats, including personal information collected by CCTV cameras.

8.1.3 In line with GDPR there are a number of general principles that local authorities must use when reviewing its use of client information and these are set out below:

(a) Lawfulness, fairness and transparency - processed lawfully, fairly and in a transparent manner in relation to individuals

(b) Purpose limitation - collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes

(c) Data minimisation - adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

(d) Accuracy - accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

(e) Storage limitation - kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals

(f) Integrity and confidentiality - processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

8.2 Collecting & using information

8.2.1 In line with GDPR principles, the council is clear that personal information should only be used where there is a legitimate reason to do so, and objections to the disclosure of confidential information shall be respected. There is a corporate Privacy Notice on the council's website which explains how we use the personal information that we collect, and also sets out how individual service areas will also use such information.

8.3 Sharing Information

8.3.1 The council is committed to using and sharing information in order to carry out its duties and it recognises the importance of maintaining confidentiality to its service users. Data sharing will be undertaken in accordance with the Information Commissioner's Office Data Sharing Code of Practice

A register of Data Sharing Agreements will be maintained by the Information Governance Officer.

8.3.2 Service Head's or responsible managers within each service area, have overall responsibility for any Information Sharing agreements into which they enter. These should be in place and reviewed regularly where information is to be shared on a large scale or on a regular basis.

8.3.3 The council supports the sharing of information internally where appropriate and where there is a business need to do so for efficient service delivery. Access to additional network resources (software / T drive access) is restricted by ICT based on requirements of individual Service Areas. Structured controls are in place to prevent access to information where that information needs to be protected. Controls are also put in place to lessen the impact of virus and malware outbreaks should such an event occur. Manager's must complete an IT ticket if permissions need to be granted to share access to folders.

8.4 Information Data Flows

8.4.1 The council will ensure that all data flows are identified and recorded on the Information Asset Register and that this is reviewed on an annual basis by each Service area. Where necessary, a Data Sharing Agreement should be set up as outlined in Section 8.3.1 above.

8.5 Data Protection Impact Assessments

8.5.1 DPIAs are an essential part of our accountability obligations. Conducting a DPIA is a legal requirement for any type of processing, including certain specified types of processing and is required when the Council uses new technologies and the processing is likely to result in a high risk to the rights and freedoms of individuals.

As outlined in the Data Protection Policy, they must be completed by Directors or Heads of Service and they must contain a description of the processing operations and the purposes, including where applicable, the legitimate interests pursued by the Data Controller; an assessment of the necessity and proportionality of the processing in relation to the purpose; an assessment of the risk to individuals; the measures in place to address risk, including security and to demonstrate that the Council complies.

Heads of Service / Directors must submit a written record of their DPIA to the Data protection and/or Information Governance Officers for the Council's records.

By considering the risks related to our intended processing before we begin, we also support compliance with another general obligation under UK GDPR: data protection by design and default.

However, DPIAs are not just a compliance exercise. An effective DPIA allows the Service area to identify and fix problems at an early stage, bringing broader benefits for both individuals and the council.

It can reassure individuals that we are protecting their interests and have reduced any negative impact on them as much as possible.

9. Compliance with the Freedom of Information Act (FOI) 2000

9.1 The Freedom of Information Act requires every public authority to adopt and maintain a Publications-Scheme which has been approved by the Information Commissioner, and to publish information in accordance with the scheme. They also have to deal with individual requests for information that give a public right of access to general information, unless an exemption applies.

9.2 The Information Commissioner's Office expects councils to make the information in this publication scheme available unless:

- it does not hold the information;

- the information is exempt under one of the FOIA exemptions or Environmental Information Regulations exceptions, or its release is prohibited by another statute;

- the information is readily and publicly available from an external website; such information may have been provided by the public authority or on its behalf. The authority must provide a direct link to that information;

- the information is archived, out of date or otherwise inaccessible; or,

- it would be impractical or resource-intensive to prepare the material for routine release. The guidance is not meant to give an exhaustive list of everything that should be covered by a publication scheme. The legal commitment is to the model publication scheme, and public authorities should look to provide as much information as possible on a routine basis.

9.3 Generally such requests need to be responded to within 20 working days and this can only be achieved if information is being well managed.

Freedom of Information

10.Compliance with the Environmental Information Regulations

10.1 The council will comply with The Environmental Information Regulations 2004 which provides public access to environmental information held by public authorities.

The Regulations do this in two ways:

- public authorities must make environmental information available proactively;
- members of the public are entitled to request environmental information from public authorities.

10.2 In addition to these legal obligations, there are two codes of practice that the council should follow, that recommend good practice for complying with the Regulations.

- the code of practice on the discharge of the obligations of public authorities under EIR (the EIR code of practice) sets out good practice recommendations for you to follow in meeting your obligations under the Regulations. It sets out the situations when you should give advice and assistance to requesters, guidelines on making information available proactively, and considerations that may affect your relationships with other public bodies or third parties.

- The section 46 code of practice covers good records management practice and the obligations of public authorities under the Public Records Act. This is relevant to the Environmental Information Regulations and the Freedom of Information Act.

10.3 The Council will aim to respond to all requests within the statutory period of 20 working days following receipt of a valid request. An extension may be sought, however, where the request is complex or voluminous. Regulation 8 of the EIR does however, allow the council to charge for making such information available provided the charge is reasonable and does not act as an obstacle to access. The Environmental Information Regulations 2004 can be viewed here.

11.Information Complaints

11.1 If someone feels that their request under the FOIA, EIR or the GDPR has not been dealt with in a satisfactory way, it will be dealt with in line with the Information Complaints Policy which is available on the council's website.

11.2 Where the complaint is not about a breach of an act or regulations we will aim to resolve the matter informally with the Service area concerned.

12. Information Request Charging/Re-use

12.1 As part of the Government's drive to ensure local Councils are fully accountable for their spending they have introduced a Transparency agenda. This is to make data more readily available to the public and enable residents to hold local Councils to account over where the money goes and how it delivers its services.

The council is committed to being as transparent as possible in how it spends tax payers' money and, as part of this, is publishing a range of information in line with the Local Government Transparency Code. However, where information is protected under the Data Protection Act or is deemed commercially sensitive then it is excluded or redacted accordingly in line with the guidance. Under the FOIA we are permitted to refuse to comply with a request if to do so would exceed the fee limit set out in the Freedom of Information and data protection (Appropriate Limit & Fees) Regulations 2004. The fee limit for public authorities is £450. This fee limit is reached if it is estimated that the time taken to carry out the activities requested would exceed 18 hours of employee time based on a £25 per hour rate. Where it is estimated that the £450 fee limit would be exceeded the requester will receive a refusal notice explaining the calculation and provide advice and assistance to, if possible, revise the request so that it remains within the fees limit or. Section 12 of the FOIA allows us to refuse requests on these grounds.

All of the information published in accordance with this code is available for re-use under the terms of the Government Open Licence for public sector information.

13.De-identification (Anonymisation & Pseudonymisation)

13.1 Confidentiality of service user information is protected when appropriate, through the use of de-identification techniques, which turn information into a form which does not identify individuals and where re-identification is not likely to take place.

13.2 There are several instances where the council will need to remove personal data from information prior to release, as follows:

- When responding to Subject access requests under the DPA;

- When proactively making information available under the Freedom of Information Act (FOIA) or the Environmental Information Regulations (the EIR);

- When responding to information requests under FOIA or the EIR and disclosing third party personal data would breach one of the data protection principles;

- When redacting information that is outside the scope of an FOIA or EIR request is the most efficient way of releasing relevant information that should be disclosed;

- When making personal data available for re-use under the Reuse of Public Sector Information Regulations (RPSI) would breach the data protection principles.

The ICO has written the following guide "How to disclose information safely."

13.3 The council does use redaction tools such as IDOX Redact within Planning and access is restricted to named individuals.

13.4 The council's Anonymisation and Pseudonymisation Policy provides further information on procedures.

14. Information Security & Transportation, Transfer and sharing of Data Policy

14.1 The council expects to protect its information assets from all threats, whether internal or external, deliberate or accidental. The Information Security Policy sets out the controls and processes that staff should adhere to. The purpose of security in an information system is to preserve an appropriate level of:

- Confidentiality: to prevent unauthorised disclosure of information

- Integrity: to prevent the unauthorised amendment or deletion of information ensuring it is authentic, accurate and complete.

- Availability – to prevent unauthorised withholding of information or resources and ensuring that authorised people can access it when they need to in the right ways.

14.2 See also the Data Sharing Code of Practice on the Information Governance page The Hub

15. Risk Management

15.1 There are significant risks in not managing information appropriately as this can have consequences for the council's reputation and its finances.

15.2 The council will provide protection by managing risks to the confidentiality, integrity and availability of information to assist our business to function effectively. Information Risk management forms a key part of the Risk Management Policy Statement & Strategy, and is embedded into council processes and functions.

16.Data Quality Assurance

16.1 In order to be able to provide excellent services for local people, it is vital that accurate quality data is available. The council must ensure that any information that is used is reliable: that the data we produce and share with other agencies is robust, and that the data provided to us by third parties, is equally assured in terms of data quality. Good quality data will contribute to good quality decisions, and thereby drive improvement in service delivery for the benefit of our local people. Data quality is therefore an integral part of the Council's service Information Governance Framework.

16.2 If an individual challenges the accuracy of their personal data, the council will consider whether the information is accurate and, if it is not, will delete or correct it. Individuals have the absolute right to have personal data rectified.

16.3 Individuals do not have the right to erasure because data is inaccurate, however, the accuracy principle requires us to take all reasonable steps to either erase or rectify inaccurate data without delay.

17. Network Management

17.1 The Council's network is segmented to protect sensitive council information systems from unauthorised access via Internet, wireless and internal based access. Secure firewalls and other controls such as Virtual Private Networks and email encryption software, are used to control remote access across the Internet. Our IT services also use other appropriate technologies e.g. secure firewalls. Virtual LANs and routers, to segregate the internal network where necessary

17.2 Secure network connection controls are in place, i.e. firewalls and routers, between the council and any other organisation's network, including the internet. The controls are configured so that computer connections and information flows are restricted in line with the council's business and security requirements.

18. Incident Management & Data Protection Breaches

18.1 The council is responsible for the security and integrity of all the information it holds and must protect this information using all means necessary, by ensuring that any near miss or actual incident, which could cause damage to the Council's assets and reputation, is prevented and/or minimised.

18.2 The council has a Data Breach Policy which outlines the process to follow should a breach or 'near miss' occur. The member of staff who discovers or receives a report of a data breach, must complete the Data Breach Notification Form and submit this to the Monitoring Officer as soon as possible, as reported breaches may need to be reported to the Information Commissioner's Office within a 72-hour timeframe.

19.Information Systems Control

19.1 An Information Asset Register (IAR) is maintained which offers improved understanding and visibility. Having this well-maintained IAR, also plays an important role in being able to demonstrate that the Council understands and protects those assets, as required under GDPR. The IAR also increases visibility of data flows which can further help to mitigate the risk of data breaches. As we share our data with third parties, GDPR places the responsibility to protect shared data on the original holder of that data. This means that if any of the third parties that we share data with are a victim of a data breach, we will be able to assess exactly what data has been compromised and what further steps we need to make to reduce any reputational or financial damage. Therefore, the IAR will help us minimise any subsequent business risks that arise from GDPR. The Information Governance Officer (IGO) will ensure that Information Systems are reviewed regularly for technical compliance with relevant security implementation standards, which are detailed in the Information Security Policy

19.2 Each Service Area has a dedicated Information Asset Owner, who is responsible for ensuring that the systems in their Services, both electronic and paper based are documented on the IAR and that they have appropriate controls and procedures in place. The Information Asset Owner will also be responsible for ensuring that where required, access is restricted to the appropriate staff and that a record of Permissions is maintained.

20.Roles & Responsibilities

20.1 Responsibilities for information governance are assigned to specific staff and this is written into their employment contracts. A training plan agreed internally, identifies two levels of training for staff; with a mandatory GDPR Data Protection course aimed at informing all levels of staff about the basic requirements of GDPR and an intermediate level of training, providing more in-depth training for managers and information champions. Guidance and information on all aspects of information governance is available on The Hub and the council's website.

20.2 **Senior Information Risk Owner (SIRO)** – The SIRO is concerned with the management of all information assets and is a senior officer familiar with information risks and leads the organisation's response. The SIRO provides board level accountability and greater assurance that information risks are addressed, fosters a culture for protecting and using information and provides a focal point for managing information risks and incidents.

20.3 **Information Asset Owner (IAO** – IAOs are concerned with the information used within their particular areas of business. They are senior individuals and their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why.

20.4 **Data Protection Officer (DPO)** – The DPO is a statutory role and is responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements.

20.5 **Information Governance Officer (IGO)** – This role has day to day responsibility for the operational procedures supporting the Information Governance framework and for the processing and dissemination of all Information Governance related requests received by the council together with subsequent enquiries.

20.6 **Data Protection/FOI/EIR Champions** – each service has nominated coordinators for Data Protection/FOI/EIR who are responsible for coordinating responses to FOI requests, EIR requests, Subject Access Requests (SARs) and requests in relation to other rights under the GDPR for their nominated areas.

20.7 **All employees** and those acting on behalf of the council are responsible for the data and information they generate. All staff will be made aware of their responsibilities and in particular those of the GDPR, FOI and EIR and the duties they place on the council as a public authority.

21.Audit

21.1 This policy, standards and procedures will be audited periodically as part of the Audit Risk Assurance (ARA) Audit Plan and any improvement or recommendations actioned by the Information Governance Officer.

22. Training & Awareness

22.1 It is important that our staff have the skills and knowledge they need to safeguard the information in their trust. A mandatory Data Protection course has been designed to ensure that

staff understand their responsibilities with regards to Data Protection & GDPR. This is first undertaken as part of the Induction process and completed annually thereafter.

22.2 Appropriate training in conjunction with this policy framework will be provided to staff.

22.3 Key staff will receive further training and procedures, applicable to their role.

23. Implementation

23.1 This Information Governance Framework is effective immediately

24.Monitoring & Review

24.1 This information Governance Policy will be monitored and reviewed on an annual basis or where there are changes to legislation or codes of practice, reporting to the Monitoring Officer and Senior Leadership Team for strategic direction and approval.

25. Useful Contacts

a. The Information Commissioner's Office via www.ico.org.uk
b. Data Protection Officer: data.protection@stroud.gov.uk
c. Freedom of Information: foi@stroud.gov.uk