Information Governance Framework

Strategy | Procedures
Policies | Resources

April 2024

Corporate Policy & Governance

Stroud District Council
Ebley Mill
Stroud
GL5 4UB

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

Contents

Using this document

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

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

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

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

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

1. Information Governance Framework

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

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

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

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

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

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

2. Information Governance Strategy

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

Valuing Our People

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

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

Making a difference

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

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

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

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

Aiming High

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

One Council

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

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

3. Roles & Responsibilities

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

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

4. Policies

4.1. Data Protection Policy

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

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

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

What is data protection?

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

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

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

Why is it important?

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

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

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

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

Responsibilities as a representative of the Council

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

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

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

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

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

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

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

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

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

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

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

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

Considerations

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

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

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

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

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

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

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

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

Overview

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

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

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

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

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

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

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

Regulation of Investigatory Powers Act 2000 (RIPA)

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

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

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

Investigatory Powers Act 2016 (IPA)

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

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

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

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

Use of Internet and social media for investigation and enforcement

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

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

Camera Locations and System Management

Overt cameras / CCTV for general monitoring may be installed:

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

Overt or covert surveillance cameras may be installed:

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

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

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

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

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

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

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

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

Sharing and disclosure of surveillance data

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

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

Routine reasons to share surveillance data include:

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

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

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

5. Procedures

5.1. Data Anonymisation

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

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

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

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

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

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

When to anonymise

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

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

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

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

Before anonymising data, you should also consider:

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

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

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

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

Examples:

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

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

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

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

How to anonymise

1) Select your anonymisation methods:

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

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

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

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

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

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

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

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

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

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

5.2. Data Breaches

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

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

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

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

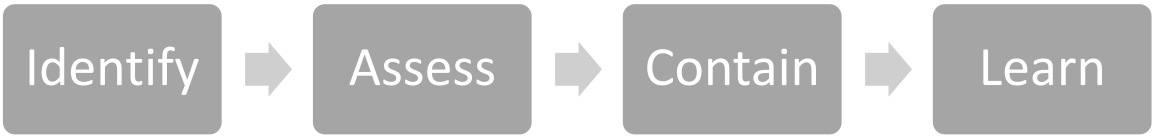
All stakeholders involved in Council matters must take responsibility for ensuring the data they process is done so fairly, securely and with due care and attention to minimise the risk of a breach. Anyone identifying or being told about a breach must report it to their line manager and the DPO as soon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

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

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

When a suspected breach is reported the relevant service area should follow the steps outlined below. Officers will not admit fault or contact data subjects without express permission of the DPO. Upon discovery, it is important to only gather information and confirm

that we will investigate. Premature actions and conclusions can lead to additional harm or exacerbate a breach. The following steps will be taken to manage a personal data breach:



Identify

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

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

Assess

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

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

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

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

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

Contain

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

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

- Can we retrieve or destroy the data?

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

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

Learn

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

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

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

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

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

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

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

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

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

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

5.4. Data Sharing

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

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

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

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

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

Ad-hoc Requests

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

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

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

Routine Requests

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

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

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

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

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

The DPO can assist officers to create suitable sharing agreements.

Data Protection Impact Assessments (DPIA)

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

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

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

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

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

Data Sharing, Transparency, and Information Requests

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

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

5.5. Individual Rights Requests

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

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

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

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

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

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

Right of access (SAR)

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

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

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

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

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

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

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

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

Right of rectification

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

Right to be informed

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

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

Right to erasure

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

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

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

Right to restrict processing and right to object

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

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

Right to data portability

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

Rights related to automated processing

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

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

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

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

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

What information is included?

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

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

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

Responding to requests

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

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

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

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

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

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

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

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

Common Exemptions and queries

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

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

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

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

5.7. Information Complaints

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

Complaint topics for iGov can include:

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

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

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

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

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

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

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

5.8. Records Retention & Management

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

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

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

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

Creation

Records must be created for a specific purpose, and we should only collect the minimum data needed for that purpose. It is recommended that anytime a service wishes to create a

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

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

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

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

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

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

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

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

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

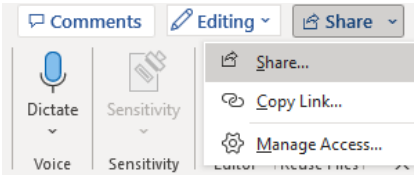
Access & Sharing

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

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

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

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



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

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

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

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

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

Retention

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

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

6. Local Government Transparency

As a local authority we publish certain information "to place more power into citizens' hands to increase democratic accountability and make it easier for local people to contribute to the

local decision-making process and help shape public services." (Local Government Transparency Code, 2015)

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

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

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

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

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

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

7. Additional Guidance

7.1. Procurement, Contracts, and International Transfers

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

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

It is not recommended to purchase or use any services or systems where data will be stored

in a jurisdiction where data protection law is less robust than the GDPR. Officers should enquire with the DPO if there are any doubts.

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

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

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

7.2. The use of Artificial Intelligence

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

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

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

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

8. Information Governance Resources, Training and Skills

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

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

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

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

9. Legislation

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

10. Glossary

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

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

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

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

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

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

Data Subject - A living individual to whom data relates.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

11. Document Control

Document Responsibility		
Name	**Document title**	**Service**
Data & Information Governance Manager	Information Governance Framework	Corporate Policy & Governance

Document Version Control			
Date	**Version**	**Issued by**	**Summary of changes**
4th April 2024	1.03	O. Chandler	Creation

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

Document Review and Approvals		
Name	**Action**	**Date**
Audit & Standards Committee	Approved	16/04/2024