Version 4.00

Data Protection Policy

www.southglos.gov.uk

South Gloucestershire Council

Version history

Version	Date	Amendments	Reviewed/Approved
V1.00	January 2009	First Version	DIG
V1.10	January 2010	Updated	DIG
V1.20	March 2011	Updated	DIG
V1.30	April 2013	Updated	DIG
V1.40	April 2014	Updated	DIG
V2.00	July 2017	Reviewed and updated	MH
V3.00	April 2018	Revision for GDPR/DPA2018	MH / DIG
V4.00	Jan 2021	Minor review and update	MH / DIG

Due Date of next review/revision: On or before Jan 2023

Author: Mike Hawke

Intranet location:

www.southglos.gov.uk/Documents/DataProtectionPolicy.pdf

Document source: Z\2Documents\1Policies\DPPolicy

Comments and Suggestions:

We welcome comments and suggestions from readers. They will help us to improve this document in later editions. Please make them to mike.hawke@southglos.gov.uk

Contents

1 Policy Summary

This policy provides South Gloucestershire Council's standards which must be maintained to comply with the UK Data Protection Act 2018 (DPA) and EU General Data Protection Regulation 2018 (GDPR), and refers to further guidance.

This document will be available to: **All South Gloucestershire Council Employees, Partners, Contractors, Agents and Elected Members.**

Key Messages

- South Gloucestershire Council (SGC) is defined as a data controller and as such all council employees, contractors and members have a responsibility for data protection.
- You must read, understand and comply with the SGC Information Governance Framework and guidance to be found on the intranet.
- Data protection applies to all the personal and "sensitive" special category data held by, and on behalf of the council. This information must be lawfully and fairly processed and where required explicit consent must be obtained and recorded.
- You must only access personal data, client records, files and folders which you "need to know" in order to do your job. Unauthorised access is a criminal offence.
- Safeguarding of people, at immediate risk of harm, over-rides data protection concerns.
- All members of the public, employees and members, as data subjects, have statutory rights including the right to know what personal information we hold about them and to have a copy of that information.
- You must complete the Annual Data Protection and Security refresher training and sign up to the Confidentiality Agreement that is contained within it.
- You must report any suspected data breach of personal or sensitive data to your Data & Information Group representative within 72 hours of becoming aware of the breach.
- Make yourself aware of the additional statutory responsibilities on the council, including the need for Privacy Notices, Data Processing Contracts, Records Management, Data Protection Impact Assessments, the SGC Data Protection Officer, RIPA (Covert Surveillance), PCI DSS (Payment Card regulations).

This is a summary of the detailed policy document please ensure you read, understand and comply with the full policy

2 Policy Statement

South Gloucestershire Council (SGC) is fully committed to compliance with the requirements of the UK Data Protection Act 2018 (DPA), the EU General Data Protection Regulation (EU) 2016/697' (GDPR), statutory guidance and other associated legislation ("the Act 2018").

The council will therefore aim to ensure that all employees, elected members, contractors, agents, consultants, or partners of the council who have access to any personal data held by or on behalf of the council, are fully aware of and abide by their duties and responsibilities under the Act 2018. Specifically in respect of:

- their responsibilities under data protection law for the protection of personal data
- the benefits of appropriate data sharing
- the necessity for good records management
- the technical and administrative controls operating in the council

3 Purpose

South Gloucestershire Council needs to collect and use certain types of information about people with whom it deals in order to perform its functions. This includes information on current, past and prospective employees, suppliers, clients, customers, service users and others with whom it communicates. The council is required by law to collect and use certain types of information to fulfil its statutory duties. In addition, it may occasionally be specifically required by law to collect and use certain types of personal information to comply with the requirements of government departments such as the Police the NHS, DWP, MoJ and other 3rd parties.

This personal information must be dealt with properly whether it is collected, recorded and used on paper, computer, or other material. There are safeguards to ensure this in the Act 2018.

The council regards the lawful and correct treatment of personal information as critical to successful operations, and to maintaining confidence between those with whom we deal and ourselves. It is essential that it treats personal information lawfully and correctly.

The purpose of this policy is to explain how the council will ensure compliance with the Act 2018. It includes organisational measures and individual responsibilities which aim to ensure that the council complies with the Data Protection principles and respects the rights of individuals. This policy provides outline measures and puts in place a structure for monitoring compliance.

Detailed procedures and guidance do not form part of this overarching policy document. The detailed guidance can be accessed via the intranet site and links to relevant documents are included within this Policy document. Other related policies are listed under Section 17.

4 Legal Context and Definitions

4.1 Data Protection Act 2018 and the GDPR

The UK Data Protection Act 2018 (DPA) and EU General Data Protection Regulation EU) 2016/679 (GDPR) governs how information about people (Personal Data) should be treated. It also gives rights to individuals whose data is held. The Act came into force on 25 May 2018 and applies to all personal data collected at any time whether held on computer or manual record. The Act is enforced by the Information Commissioner's Office.

The Act 2018 makes a distinction between personal data and special category "sensitive" personal data. Special category personal data is subject to stricter conditions of processing.

Personal data means any information relating to an identified or identifiable living individual, where an "Identifiable living individual" means a living individual who can be identified, directly or indirectly, in particular by reference to:

A) an identifier such as a name, an identification number, location data or an online identifier, or

B) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

Special Category 'Sensitive' personal data is defined as personal data revealing:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health data
- Sex life or sexual orientation
- Criminal proceedings or convictions

A **Data Subject** is the identified or identifiable living individual to whom personal data relates.

A **Data Controller** is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

A **Data processor** is any person who processes personal data on behalf of the controller (other than a person who is an employee of the controller).

Processing in relation to personal data, means an operation or set of operations which is performed on personal data, or on sets of personal data, such as:

(a) collection, recording, organisation, structuring or storage

(b) adaptation or alteration

(c) retrieval, consultation or use

(d) disclosure by transmission, dissemination or otherwise making available

(e) alignment or combination, or

(f) restriction, erasure or destruction

The GDPR (Article 5) contains 6 principles for processing personal data with which organisations must comply.

The **data protection principles** require that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')

b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

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

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

e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, with due regard to the rights and freedoms of the data subject ('storage limitation')

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

As the controller we are responsible for, and be able to demonstrate compliance with, the above data protection principles (‘accountability’).

Fairly means that the data subject has been provided with, or had the following information made available to them: the identity of the data controller, the purposes for which the data is to be processed, the legal basis that enables the council to process the data, who we may share the data with, how long we will keep the data, the rights of the data subject and any further information which is necessary in the circumstances to allow the processing to be fair.

Fairness information is the information that must be provided in a clear and transparent form to the data subject in order to ensure that the processing is fair.

This information is provided in our Privacy Statement and additional fair processing statements for specific services.

Data subject rights are to:

- Be informed that processing is being undertaken
- Access to one's personal information – Subject Access Request (SAR)
- Request rectification – the correction of incorrect information
- Request erasure / deletion of their records (right to be forgotten
- Restriction – restricting the processing of personal data
- Portability
- Object to processing
- Object to automated decision making & profiling
- Complain to the Information Commissioner's Office

The DPA and GDPR is fully retrospective in that it applies to information collected prior to the Act coming into force.

Abbreviations:

DIG – Data & Information Group
DP – Data Protection
DPA – Data Protection Act 2018
GDPR – General Data Protection Regulation
FOI – Freedom of information
DPO - Data protection Officer
IGCO – Information Governance Compliance Officer

4.2 Other related legislation

There is significant legislation across the public sector in relation to data and information governance, including:

Human Rights Act 1998
Freedom of Information Act 2000
Environmental Information Regulations 2004
Computer Misuse Act 1990
Privacy and Electronic Communications Regulations 2003
Education (Pupil Information) Regulations 2005
Children Act 2004
Digital Economy Act 2017

Common law duty of confidentiality

Employer's common law duty to employees to maintain a relationship of mutual trust and confidence.

4.3 Further definitions and abbreviations

Caldicott Principles

The following are derived from the UK Caldicott Guardian Council's 'A Manual for Caldicott Guardians' as published December 2020:

Principle 1: Justify the purpose(s) for using confidential information

Every proposed use or transfer of confidential information should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian.

Principle 2: Use confidential information only when it is necessary

Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.

Principle 3: Use the minimum necessary confidential information

Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.

Principle 4: Access to confidential information should be on a strict need-to-know basis

Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.

Principle 5: Everyone with access to confidential information should be aware of their responsibilities

Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.

Principle 6: Comply with the law

Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.

Principle 7: The duty to share information for individual care is as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users within

the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Principle 8: Inform patients and service users about how their confidential information is used.

A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.

5 Scope

5.1 Context of this policy

5.1.1 This policy applies to all councillors, committees, services, partners, employees of the council, contractual third parties and agents of the council who has access to information held or processed by SGC.

5.1.2 The policy describes the correct handling personal and special category data in order to comply with the current data protection legislation and related statutes.

5.1.3 The policy should be read in conjunction with the Employee Code of Conduct and Members' Code of Conduct and codes of conduct (e.g. Health and Care Professions Council) governing the professional conduct and standards of staff in certain occupations.

5.1.4 The policy is supported by other corporate policies including Freedom of Information and Environmental Information Requests, Subject Access Requests, Corporate Records Management, ITD Security and Acceptable Use, Email best practice and various Human Resources Policies including Criminal Records Bureau Staff checks (Disclosure and Barring Service) Policy and Procedures.

5.1.5 This policy may be supported by Departmental policies and agreements and information sharing protocols for specific areas of work.

5.1.6 This policy may be supported by procedures and guidance for specific areas of work or specific data protection issues, which can be obtained from the Information Governance Framework.

5.1.6 This policy replaces the previous data protection policy.

5.2 Personal data held

5.2.1 This policy applies to all processing of personal data held by the council. This includes:

- Personal data processed by the council.

- Personal data controlled by the council but processed by another organisation, on the council's behalf (for example private sector contractors; and Service Level Agreements with voluntary sector organisations).
- Personal data processed jointly by the council and its partners

5.2.2 The policy does not cover personal data held by schools or Parish Councils which are data controllers in their own right.

5.2.3 This policy applies to personal data processed by Elected Members in their capacity as councillors of South Gloucestershire Council. For political activities and campaigning for elections each Elected Member should be covered by their political party. For their constituency responsibilities, including individual casework, Elected Members are individually responsible and will need to continue to register with the ICO annually as a Controller in their own right for these limited purposes.

5.2.4 Personal data held by the council may be held in many forms including:

- Database records
- Computer files
- Emails
- Paper files
- CCTV and video recordings
- Sound recordings
- Photographs
- Microfiche and film
- Website
- Mobile phones

5.2.5 Data subjects may include:

- current, past and prospective employees
- suppliers
- clients
- customers
- service users
- others with whom the council communicates

5.2.6 Deceased individuals are not classified as data subjects under the DPA and therefore processing of this type of data is outside the scope of this policy. However, the Caldicott 2 review has come up with a practical (not legal) definition which the ICO has accepted, which is of Personal Confidential Data (PCD) which includes the DPA definition of Personal Data but is adapted to include dead as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' – and so accords protection to information relating to deceased people which was given in confidence.

6 Responsibilities and Penalties

6.1 Organisational Responsibilities

6.1.1 South Gloucestershire Council is a data controller under the Data Protection Act 2018 & the GDPR.

6.1.2 The council as an organisation is responsible for compliance with the DPA and therefore ultimate responsibility rests with the Chief Executive of SGC. Failure to comply with DPA may result in criminal prosecution.

6.1.3 The Senior Information Risk Owner (SIRO) for Data Protection is the Director of Resources & Business Change.

6.1.4 The statutory role of Data Protection Officer (DPO) has been assigned to the Head of Legal, Governance and Democratic Services.

6.1.5 The Information Governance Compliance Officers will support the DPO and, together with the members of the Data & Information Group (DIG), also be responsible for the day to day compliance with the DPA and will give advice and legal assistance where necessary in the implementation of this policy.

6.1.6 The Caldicott Guardians are the Director of Public Health and the Deputy Director of Public Health.

6.2 Individual Responsibilities

6.2.1 Every employee must comply with this policy. Failure to comply with the policy may result in disciplinary action which could include dismissal.

6.2.2 Each Elected Member must comply with this policy when using personal data controlled by the council.

6.2.3 All contractors/ service providers must comply with the policy when using personal data supplied to / held by the council to facilitate the Commissioned Service being provided.

6.2.4 It is a criminal offence to:

- Unlawfully obtain personal data, includes accessing personal data held by the council for other than specific council business, or to procure the disclosure of personal data to a third party. It is a further offence to sell such data.

- Re-identification of de-identified personal data

- Alteration of personal data (alter, deface, block, erase, destroy or conceal) to prevent disclosure

6.2.6 Employees who access or use personal data held by the council for their own purposes will be in breach of relevant policies of the council, including but not limited to the Employee Code of Conduct, Social Media Policy, ITD Security Policy and subject to disciplinary action, which could include dismissal, and may also face criminal proceedings.

7 Purposes of Processing Personal Data and Fairness

7.1.1 The council will collect and process personal data only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.

7.1.2 The council will also establish the lawful conditions for processing the individual's personal data, such as in association with:

- A contract
- A legal obligation
- The Vital interest of the individual or another person
- The public interest or an authority vesting in the council
- The legitimate interests of the council, providing the task involved is not directly related to the provision of a service to the public

If none of the above conditions apply and the processing is required the council will obtain the consent, which must not be implied, from the individual before processing their personal data. The consent must be freely given, specific, informed and an unambiguous indication of the individual's wishes by which the individual, by a statement or by a clear affirmative action, signifies agreement to the processing of the personal data.

7.1.3 When special category 'sensitive' data is collected, the council will also need to ensure a secondary condition is also met from within Article 9 (2) of the GDPR (processing of special categories of personal data). Again, if none of the conditions apply and the processing is required the council will obtain the explicit written consent from the individual before processing their special category personal data. If in doubt please consult with the Data Protection Officer.

7.1.4 The council will ensure that all individuals, whose personal details are processed, are provided with, or have the following information made available to them: the identity of the data controller, the purposes for which the data is to be processed, the legal basis that enables the council to process the data, who we may share the data with, including the likely recipients of the information - whether the recipients are internal or external to the council, how long we will keep the data, the rights of the individual and any further information which is necessary in the circumstances to allow the processing to be fair.

7.1.5 Whenever possible this information will be provided when personal data is first collected, whether written or verbal, or if circumstances don't allow this within one month of the council obtaining the personal data.

7.1.6 When personal data is to be used for a new purpose then the fairness information will be provided to the data subject again and if necessary a new consent will be sought.

7.1.7 Individuals are free to ask for more details about how their personal data is being used at any time, they may also elect to exercise their other data subject rights, but granting these right will always be subject to our scrutiny and agreement. If unhappy about how their data is used individuals may also make a complaint, initially to the council and to the ICO.

7.1.8 Any person whose details (including photographs) are to be included on the council's public website will be asked to give explicit written consent. At the time the information is included or collected, all such individuals will be properly informed about the consequences of their data being disseminated worldwide.

7.1.9 The council will use exemptions under the DPA / GDPR where necessary, for example where sharing information with the police when it is necessary for a police investigation. The council will respond to properly submitted applications under Schedule 2, sections 2 and 3 of the DPA from the Police and other relevant agencies for information that will assist in the prevention and detection of crime and for the collection of taxes, duties, levies and other charges.

7.1.10 In accordance with good practice the council will share information where appropriate in accordance with formal data sharing arrangements and in accordance with the DP principles.

8 Data Quality, Integrity and Retention

8.1.1 Personal data held will be relevant to the stated purpose and adequate but not excessive.

8.1.2 The council will ensure, as far as is practicable, that the information held is accurate and up-to-date.

8.1.3 If personal data is found to be inaccurate, this will be remedied as soon as possible.

8.1.4 Personal information, such as contact details, may be shared within the council where it is necessary to keep records accurate and up-to-date, and in order to provide individuals with a better service.

8.1.5 Records may include professional opinions about individuals but employees will not record any personal opinions about individuals.

8.1.6 The council's use of personal data will comply with the Corporate Records Management Policy and Retention Schedules covering every type of council record.

8.1.7 Information will only be held for as long as is necessary after which the details will normally be deleted or fully anonymised so that the individual cannot be identified. Where details of individuals are stored for long-term archive or historical reasons, and where it is necessary to retain the personal detail within the records, it will be done within the requirements of the legislation.

8.1.8 Redundant personal data will be destroyed using the council's procedure for disposal of confidential waste and in accordance with departmental retention schedules.

9 Security

Any inappropriate, unauthorised access of data, use or misuse of data or failure to comply with ITD security arrangements and policies may result in disciplinary action, including dismissal.

9.1.1 The council will implement appropriate technical and organisational security measures so that unauthorised staff and other individuals are prevented from gaining access to personal information.

9.1.2 An employee must only access personal data they need to use as part of their job. Inappropriate or unauthorised access will not be tolerated.

9.1.3 The council has an ITD Security Policy which applies to electronic systems containing personal data. The Security Policy is managed by the Head of ITD. All ITD security incidents should be reported to the ITD Helpdesk.

9.1.4 All other information security incidents (including data breaches), however minor, should be reported via the process detailed on the Information Governance intranet site immediately after becoming aware of the incident.

9.1.5 All managers and staff within the council's departments will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure.

9.1.6 Manual files and other records or documents containing personal/sensitive data will be kept in a secure environment and accessed on a need-to-know basis only.

9.1.7 Personal data held on computers and computer systems will be installed with user-profile type password controls, encryption and where necessary, audit and access trails to establish that each user is fully authorised. Personal data should not be held on unencrypted electronic devices or media.

9.1.8 Security arrangements will be reviewed regularly, any reported breaches or potential weaknesses will be investigated and, where necessary, further or alternative measures will be introduced to secure the data.

9.1.9 Employees who process personal data out of the office (e.g. off site, on client premises, at home) can only do this with the express approval of their senior manager. Access to personal data outside of the council should not be attempted using unsecured access systems (this includes via mobile networks outside of UK unless the network has been checked in advance to be compliant under data protection law).

9.1.10 System testing will only be carried out using personal data where sufficient safeguards are in place and will not be undertaken on live databases accessing live personal sensitive data.

9.1.11 Personal data will not be transferred outside the UK without the approval of the Head of ITD and Data Protection Officer.

10 Data Subjects Rights

10.1.1 The council will ensure that the rights of people about whom personal information is held can be fully exercised under the Act.

10.1.2 The right to access records – Subject Access Request (SAR)

An individual can request to see all the personal data that the council holds about them or someone they have a legal responsibility for. Full details can be found here - Subject Access Request Policy and Guidance. Please note that our response times to these requests, and the other types of requests below, is **one calendar month**, so employee response to such requests must be actioned with the appropriate priority. Servicing these requests continue to be free.

Some requests may result in a combination of personal and non-personal information. In such cases the Freedom of Information Act 2000 will also need to be applied, as the legislation governs the disclosure of non-personal information held by the council.

If in any doubt, or a request is considered particularly sensitive/complex please ensure legal advice and support is sought from the Data Protection Officer before coming to a decision and disclosing the requested information.

10.1.3 The right to request rectification – the correction of incorrect information

If an individual identifies that information we hold about them is incorrect SGC must investigate and, if the law allows, correct the inaccuracy. However, in many cases SGC will be required to keep the old record by law and will instead append a note to the record advising of the suggested correction.

10.1.4 The right to request erasure / deletion of their records (right to be forgotten)

An individual can request that we delete records we hold about them. However, in many cases SGC will be required to keep the record by law and will instead append a note to the record advising that the request was made but declined.

10.1.5 The right to restriction – restricting the processing of personal data

When an individual requests that we rectify or delete records we hold about them we are obliged to cease processing the record. However, in many cases SGC will be required to continue processing the record by law and will instead append a note to the record advising that the request was made but declined.

10.1.6 The right to portability

An individual can request that we transfer their personal data records to another data controller in a machine-readable form. This is highly unlikely to occur in normal council business, but in reality will take the form of a SAR provided in electronic format such as a pdf, word or excel file.

10.1.7 The right to object to processing

An individual can object to SGC processing their personal data and we could be obliged to do this. However, in many cases SGC will be required to continue processing the record by law and will instead append a note to the record advising that the request was made but declined.

10.1.8 The right to object to automated decision making & profiling

An individual should not be subject to automated decision making unless authorised by UK law or SGC has explicit consent. As SGC does not in general use profiling or automated decision making unless it is acting under statue this is again unlikely to apply.

10.1.9 The right to complain to the Information Commissioner's Office

If an individual has cause for complaint about how their personal data has been processed by the council or one of our partners / contractors they must be advised of their right to complain to the Information Commissioner's Office (ICO). SGC provides the full contact details for the ICO via our Privacy Statement.

11 Disclosure and Sharing

11.1 Third party access to information

11.1.1 Where a request for personal data is made by a third party on behalf of the data subject it shall be treated as a subject access request. Evidence is required that the third party is entitled to act in this way, such as a written statement from the data subject or an enduring power of attorney. Appropriate professionals may need to be consulted before a decision to release the personal data is made.

11.1.2 Occasionally third party information may form part of the data extracted in response to a subject access request. In deciding whether to release this information, the council will consider the following:

- any duty of confidentiality owed to the third party
- attempts to get consent from the third party
- any express refusal of consent from the third party
- the third party's expectations with respect to that data

11.1.3 When a request for personal data is made by a third party and not on behalf of the data subject, the council shall consider the request under Freedom of Information as well as DPA. It shall consider whether releasing the personal data would breach any of the DP principles and in particular whether any exemptions under DPA apply. Employees should consult with their departmental representative as per the Information Governance Intranet

site. Personal information will not be shared with third parties unless specifically allowed for in law and justified in the specific situation.

11.1.4 The Freedom of Information policy deals with requests for information about third parties, and information will be withheld where disclosing it would breach any of the DP principles. Where a requester does not state a specific reason for requesting the information then the FOI policy should be followed. A response to an FOI request must not take into account the reasons behind the request.

11.1.5 When there is a specific reason for requesting the information, an exemption under DPA may apply. Examples are where information is required for the prevention or detection of crime, apprehension or prosecution of offenders or assessment or collection of tax.

11.1.6 If an appropriate exemption under DPA does apply so that the DP principles will not be breached, the council will usually comply with the request. If the council determines that it cannot comply with the request the legal reasons for doing so, including the considerations and outcomes of any legal 'tests', will be advised to the requestor and documented within Respond.

11.2 Information sharing

11.2.1 The council recognises the need to share personal and sensitive data with other partner organisations in order to safeguard the vulnerable and provide effective and efficient services. The ICO provides extensive guidance on this subject – ICO Code of Practice.

11.2.2 The council has also produced Information Sharing guidance and appendix 2 provides an Information Sharing Agreement (ISA) template.

11.2.3 The council has signed protocols on information sharing across Gloucestershire, Avon and Wiltshire authorities, with the NHS, the Police, with public and private organisations. The sharing of personal data will comply with the standards set out in these protocols, which where relevant, includes the Caldicott Principles.

11.2.4 Guidance on Research Governance can be found on the Information Governance intranet site which should be used where people are requesting access to information as part of a research exercise.

11.2.5 The council promotes information sharing where it is in the best interests of the data subject. However, personal sensitive data will not be shared unless it is in connection with the primary purpose for which the information was collected, or the data subject has explicitly given their permission for the information to be shared for this purpose, or another legal provision (DPA exemption exists) to allow the sharing such information.

11.2.6 The council will ensure that supporting processes and documentation are made available to professionals so that they understand how to share information safely and lawfully.

11.2.7 Where an employee acting in good faith has shared information in accordance with these supporting processes and documentation, they shall not normally be subject to disciplinary action under section 6.2.4 hereof.

11.2.8 Sharing large sets of information, or recurrent regular sharing shall be carried out under written agreement to ensure the continued compliance with the DPA and that additional safeguards can be considered and put in place.

11.3 Contractual and partnership arrangements

11.3.1 When the council enters contractual or partnership arrangements which involve the processing of personal data, a written agreement will specify which party is data controller or whether there are joint data controller arrangements. Where a third party is processing personal data and information on behalf of the council, a written contract will be put in place. Specific care should be taken in respect of services provided online and via 'the cloud'.

11.3.2 Where the council remains as data controller, it will take steps to ensure that the processing by its contractors and sub-contractors will comply with DPA. Contractors will not be able to sub-contract Data Processing without the explicit written permission of the council. Officers will take reasonable steps to ensure that data processing by third parties is regularly monitored to ensure DPA requirements are being met.

11.3.3 Where two or more controllers jointly determine the purposes and means of processing personal data, they will be known as 'joint controllers'. They shall, via a transparent documented arrangement, determine their respective responsibilities to ensure the partnership complies with the Data Protection legislation, in particular regarding how the rights of their data subjects will be met and managed. Unless their respective responsibilities are determined by UK law. The arrangement should also include a single point of contact for data subjects.

11.3.4 All contractors who are users of personal information supplied by the council will be required to confirm that they will abide by the requirements of the Act to the same standard as the council with regard to information supplied by the council. Staff should obtain advice from the Data Protection Officer as necessary.

11.3.5 All contractors, consultants, partners or agents of the council must ensure that they and all of their staff who have access to personal data held or processed for or on behalf of the council, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the Act. Any breach of any provision of the Act will be deemed as being a breach of the contract between the council and that individual, company, partner or firm. The council shall take reasonable steps to ensure regular monitoring of contracts and specifically the security of data being processed on its behalf.

11.3.6 Any observed or suspected security incidents or security concerns should be reported to the council.

11.3.7 All contractors, consultants, partners or agents of the council must allow data protection audits by the council of data held on its behalf if requested in line with these contractual arrangements.

11.3.8 All contractors, consultants, partners or agents of the council must indemnify the council against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation, providing the events are not as a result of non-compliance with the DPA 2018.

12 ICO Data Protection Fee

12.1.1 The council, as a Data Controller, is registered as such with the Information Commissioner under registration number Z5077191.

12.1.2 The Data Protection Officer is responsible for submitting this data protection registration to the Information Commissioner's Office on an annual basis following a review by the Data & Information Group (DIG).

12.1.3 The information we need to provide is:

- Our name and address as a controller
- The number of people that make up our organisation (i.e. greater than 250)
- Name and contact details of the following people:
    - The person completing the registration process
    - Our data protection officer (DPO)

12.1.4 The council also supports three further data protection registrations for the Electoral Registration Officer for South Gloucestershire (Z4854602), Superintendent Registrar of Births, Deaths and Marriages for South Gloucestershire (Z6929484) and South Gloucestershire Youth Offending Team (Z4879326).

12.1.5 Processing of personal data by Elected Members is covered by the council's main corporate data protection registration in respect of information held by the council.

12.1.6 Elected Members who process personal data obtained by them for constituency or political purposes are now exempt from paying a fee to the Information Commissioner's Office.

12.1.7 If we fail to register and pay the appropriate Data Protection fee we will receiving a reminder explaining when we need to pay. If we don't then pay, or explain why we are no longer required to pay a fee, we will issue a notice of intent 14 days after expiry. We then have 21 days to pay or make representations. If we do not pay or fail to notify the ICO that we no longer need to pay, we may be issued with a fine of up to £4,350 (150% of the top tier fee.)

13 Records of Processing Activities

The council maintains a record of processing activities of each service under our responsibility. This is an enhanced version of our Information Asset Register and contains the following information that enables us to comply with this requirement:

(a) Our name and corporate contact details, together with the contact details of our Data Protection Officer.

(b) The purposes of processing the personal data

(c) A description of the categories of data subjects and of the categories of personal data

(d) The categories of recipients to whom the personal data have been or will be disclosed including, where applicable, recipients in third countries or international organisations

(e) Details of suitable safeguards if the data is transferred outside the UK.

(f) Via our Records Retention Schedules the envisaged time limits for erasure of the different categories of data

(g) A general description of the technical and organisational security measures in place to protect this data – it should be noted that access for security reasons to such data will be extremely limited.

Similarly our data processors are expected to maintain a record of all categories of processing activities carried out on our behalf. This record contains:

(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable the data protection officer.

(b) the categories of processing carried out on behalf of each controller;

(c) Details of suitable safeguards if the data is transferred outside the UK.

(d) A general description of the technical and organisational security measures in place to protect this data – it should be noted that access for security reasons to such data will be extremely limited.

The council or our data processors may be requested to make the records available to the ICO for inspection upon request. Therefore, it is essential that the DIG departmental representatives and the Information Asset Owners and Administrators review and update at least annually. However, when the council plans to carry out new processing the relevant records must be kept up to date. Therefore, the manager responsible will inform the Data Protection Officer in good time to ensure the relevant records are amend (if necessary) within 28 days of processing beginning.

Please note elected members are not required to maintain records of their processing activities unless the processing is likely to:

- result in a risk to the rights and freedoms of data subjects
- regular rather than occasional
- include special categories of data, including personal data relating to criminal convictions and offences.

14 Subject Access Requests and Data Protection Complaints

14.1.1 The first point of contact for data subjects (applicants) should be the service area or division which holds their data or is offering a service to them. Matters should be resolved at a local level as quickly and effectively as possible with Officers and Managers to resolve complaints and run-on data requests.

14.1.2 Subject access requests and data protection complaints should be addressed to the following places:

Complaints and FOI Team
Department for Children, Adults and Health
PO Box 1955
Bristol BS37 0DE e-mail: CAHFeedback@southglos.gov.uk

Complaints and FOI Team
Departments for Environment and Community Services and Chief Executive & Corporate Resources
PO Box 1954
Bristol BS15 0DD e-mail: ECSFeedback@southglos.gov.uk

14.1.3 Complaints about the council's processing of personal data and rights under the Data Protection Act 2018, the GDPR and associated legislation will be dealt with in accordance with the relevant Policy. Complaints will be fully dealt with after a formal review. The clarification and review procedure contained in the council's Freedom of Information and Environmental Requests Policy and Procedures should be used when dealing with reviews under this policy (Data Protection) and for Freedom of Information and Environmental Information requests.

14.1.4 Under the DPA the data subject has a specific right to complain to the ICO if they feel the council is not processing their data lawfully. Data subject are informed how to contact the ICO during the Privacy Statement process via the following means:

For independent advice about data protection, privacy and data sharing issues, you can contact the Information Commissioner's Office (ICO) via their contact page or call them on 0303 123 1113

14.1.5 The council will respond promptly and fully to any request for information about data protection compliance made by the Information Commissioner's Office.

14.1.6 The council will comply with any Information Commissioner Information Notice (to provide answers and information to the Commissioner) or Enforcement Notice (for failure to provide answers or information or for a breach of the Act) sent to the council by the Information Commissioner. The Commissioner can also carry out audits, prosecute individuals and organisations and report concerns to parliament. The original or copies of Notices should be sent to The Data Protection Officer, Legal Services (DPO@southglos.gov.uk) for advice and support.

15 ICO enforcement

The Information Commissioner has various enforcement powers at her disposal ranging from inquiries into data breaches, Information Notices, Assessment Notices, Enforcement Notices, powers of physical entry and inspection and, ultimately, Penalty notices and prosecution.

Penalty notices or monetary penalties (fines) may be served for non-compliance with the DPA and or serious data breaches. There are two levels as follows:

The “higher maximum amount” is 20 million Euros

The “standard maximum amount” is 10 million Euros

The maximum amount of a penalty in sterling will be determined by applying the spot rate of exchange set by the Bank of England on the day on which the penalty notice is given.

The “higher maximum” will apply to very serious and or damaging data breaches and fundamental failure to comply with the fundamentals of the DPA ideals.

All fines are made public by the Commissioner and the Chief Executive of the offending organisation is usually asked to make a formal undertaking to put in place effective measures and remedies.

If the organisation disputes the fine, it can appeal to the First-Tier Tribunal within 28 days of being informed of the Monetary Penalty Notice.

16 Implementation

16.1.1 The responsibility for implementation of this policy rests with the Chief Executive, the Senior Leadership Team (SLT), the Senior Information Risk Officer, the Data & Information Group (DIG) and the Data Protection Officer.

16.1.2 The council will ensure that:

- Everyone managing and/or handling personal information understands that they are contractually responsible for following good data protection practice
- Everyone managing and/or handling personal information is appropriately trained to do so
- Everyone managing and/or handling personal information is appropriately supervised

- Anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, is given advice as necessary
- Queries about handling personal information are promptly and courteously dealt with
- Methods of handling personal information are regularly assessed and evaluated
- Performance with handling personal information is regularly assessed and evaluated
- Employees are aware of the action required in the event of a Data Breach.

16.1.3 On joining the council, employees are required to undertake training on Data Protection and ITD Security as part of their induction. They will not be allowed to use SGC's network until successfully completing the training and achieving at least 80% in the assessment.

16.1.4 The Data & Information Group (DIG) works with the departments to maintain the on-going programme of annual training and awareness to maintain a high level of understanding of Data Protection and security among all staff and to communicate any legal or policy changes that occur.

16.1.5 Supporting procedures for this policy have been created and are maintained within the Information Governance Framework, Policy and Guidance pages that are available to all users. Appropriate levels of consultation takes place at review time before DIG approve the changes for implementation.

16.1.6 Data Protection audits are regularly carried out by internal audit (external audits may be commissioned if required) in order to monitor compliance with the DPA and this policy.

17 Other related policies

This policy should be interpreted and applied in relation to other related policies. Breach of these policies will automatically breach this policy and this is likely to contravene the DPA and other legislation. These related policies include, but are not limited to, the following and such other policies as are adopted by the council from time to time:

1. ITD Security Policy
2. Email Best Practice Guidelines
3. Subject Access Policy and Procedures
4. Corporate Records Management Policy
5. Record Retention Schedules
6. Information Asset Owners and Administrators Guidance
7. Information Asset Register
8. Use of Images Policy
9. CCTV Protocols
10. Freedom of Information and Information Access Policy and Procedures
11. RIPA Surveillance Policy
12. Social Media Policy
13. Data Sharing Agreements, Protocols and Contracts (various)
14. National, Regional, Corporate and Departmental Policies and Procedures

For further information please see our Polices and Guidance pages

18 Monitoring and Review

18.1 The implementation and effectiveness of this policy will be monitored and reviewed by the Data & Information Group.

18.2 Reports on data protection and the operation of this policy will be made to Chief Officers Management Team as required.

18.3 This policy will be reviewed at not more than 2-yearly intervals.

18.4 Any comments about this policy should be addressed to the Information Governance Officer or departmental members of the Data & Information Group (DIG).