Version 2.0

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

Due Date of next review/revision: On or before July 2018

Author: Mike Hawke

Intranet location:

Document source: Z\2Documments\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

Table of Contents

1 Policy Statement

South Gloucestershire Council is fully committed to compliance with the requirements of the Data Protection Act 1998. 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.

2 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 and also to comply with the legal requirements of the Government. 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 Data Protection Act 1998.

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 Data Protection Act 1998. 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 15.

3 Legal Context and Definitions

3.1 Data Protection Act 1998

The Data Protection Act 1998 (DPA) 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 1 March 2000 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.

The DPA makes a distinction between personal data and "sensitive" personal data. Sensitive personal data is subject to stricter conditions of processing.

Personal data is defined as data relating to a living individual who can be identified from the data and other information which is in the possession of, or is likely to come into the possession of the data controller. This includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

Sensitive personal data is defined as personal data consisting of information as to:

Racial or ethnic origin;
Political opinion;
Religious or other beliefs;
Trade union membership;
Physical or mental health or condition;
Sexual life;
Criminal proceedings or convictions.

A **Data Subject** is an individual who is the subject of the data.

A **Data Controller** is an organisation, or person that determines the purposes for which and the manner in which any personal data is to be processed.

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

Processing means obtaining, recording, viewing, holding or carrying out any operation on data and includes organisation, alteration, retrieval, disclosure and destruction of the data.

The DPA contains 8 principles for processing personal data with which organisations must comply.

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

1) Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;

2) Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;

3) Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;

4) Shall be accurate and where necessary, kept up to date;

5) Shall not be kept for longer than is necessary for that purpose or those purposes;

6) Shall be processed in accordance with the rights of data subjects under the Act;

7) Shall be kept secure i.e. protected by an appropriate degree of technical and organisational security;

8) Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

Fairly means that the data subject has been provided with, or had the following information made available to him: the identity of the data controller, the purposes for which the data is to be processed 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 to the data subject in order to ensure that the processing is fair. This information is provided in Fair Processing Statements and Privacy Notices.

Data subject rights are:

The right to be informed that processing is being undertaken.
The right of access to one's personal information.
The right to prevent processing in certain circumstances.
The right to rectify, block or erase information which is regarded as wrong information.
The right to have decisions reviewed where they have been made automatically.
The right to object to receiving marketing information.

The data protection definitions have now been subject to interpretation by the courts. For examples the 'Durant' case decided that personal data should be 'significantly biographical' and did not include incidental mentions of people in documents in which no other information about them was included.

Each data controller has a responsibility to notify the Information Commissioner about the processing of personal data undertaken by that organisation. These notifications are made available in a public register. It is an offence to process personal data when not notified or where the notification is inaccurate.

The Data Protection Act 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
FOI – Freedom of information
DPO - Data protection Officer
IGCO – Information Governance Compliance Officer

3.2 Other related legislation

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

EC Data Protection Directive (95/46/EC)
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

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

3.3 Further definitions and abbreviations

Caldicott Principles

The following are derived from the UK Caldicott Guardian Council's 'A Manual for Caldicott Guardians 2017':

1. Justify and document the purposes for recording and/or sharing information. Make sure these are regularly reviewed by the guardian.
2. Only use and share information when absolutely necessary.
3. Use the minimum information required for the purpose - anonymising or removing as much personal/sensitive information as possible.
4. Only access information with consent or on a strict 'need to know' basis, where there is a legal requirement or public/vital interest justification.
5. Ensure awareness and understanding of everyone's responsibilities to maintain confidentiality including understanding & complying with law, including Data Protection, Human Rights and common law of confidentiality.
6. Only use information for the purpose(s) originally agreed at the time of disclosure. If later required for another purpose, the recipient must confirm appropriateness with the supplier and/or subject. Access controls and data flows may also need to be split to safeguard the data.
7. The duty to share information can be as important as the duty to protect patient information.

4 Scope

4.1 Context of this policy

4.1.1 This policy applies to all the Staff, Contractors and Members that use personal data in support of their work on behalf of the council.

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

4.1.3 The policy links with other corporate policies including Freedom of Information and Information Access Policy, Records Management Policy, ICT

Security Policy, Email and Internet Use Policies, Human Resources Policies, Criminal Records Bureau Staff checks (Disclosure and Barring Service) Policy and Procedures.

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

4.1.5 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 intranet site.

4.1.6 This policy replaces the previous data protection policy.

4.2 Personal data held

4.2.1 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

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

4.2.3 This policy applies to personal data processed by Elected Members in their capacity as Councillors of South Gloucestershire Council and their constituency responsibilities. For political activities and campaigning for elections each Elected Member is individually responsible and may need to notify with the Information Commissioner personally for these limited purposes.

4.2.4 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

4.2.5 Data subjects may include:

- current, past and prospective employees
- suppliers
- clients

- customers
- service users
- others with whom the Council communicates

4.2.6 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.

5 Responsibilities and Penalties

5.1 Organisational Responsibilities

5.1.1 South Gloucestershire Council is a data controller under the Data Protection Act 1998

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

5.1.3 The Senior Information Risk Owner for Data Protection is the Director of Corporate Resources.

5.1.4 Responsibility for day to day compliance with DPA is delegated to Legal, Governance and Democratic Services together with members of the Data & Information Group (DIG)

5.1.5 The Information Governance Compliance and Data Protection Officer responsibilities have been assigned to the Legal Services section within the Chief Executive and Corporate Resources (CECR) Department who will give advice and legal assistance where necessary in the implementation of this policy.

5.1.6 The Caldicott Guardian role has been identified and resides for the Council within the Children, Adults and Health Department.

5.2 Individual Responsibilities

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

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

5.2.3 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.

5.2.4 It is a criminal offence to access personal data held by the Council for other than Council business, or to procure the disclosure of personal data to a third party.

5.2.5 It is a further offence to sell such data.

5.2.6 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, ICT Security Policy and subject to disciplinary action, which could include dismissal, and may also face criminal proceedings.

6 Purposes of Processing Personal Data and Fairness

6.1.1 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.

6.1.2 Wherever possible the Council will obtain the individual's consent for processing of their personal data. The consent must be free and informed and may be changed at any time.

6.1.3 When sensitive data is collected, the Council will obtain the individual's explicit consent for this processing.

6.1.4 In cases where consent cannot be obtained, or to obtain consent is not appropriate, the Council will ensure that another condition of processing (as detailed in schedules 2 or 3 of the DPA) is met. These include protecting the vital interests of the data subject, meeting a legal obligation or for the prevention or detection of crime. This includes the National Fraud Initiative under the Audit Commission Act 1998.

6.1.5 The Council will, as far as is practicable, ensure that all individuals whose details are processed are aware of the way in which that information will be held, used and disclosed. Individuals will, where possible, be informed of the likely recipients of the information - whether the recipients are internal or external to the Council.

6.1.6 This information will be provided when personal data is first collected, whether written or verbal.

6.1.7 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.

6.1.8 People are free to ask for more details about how their personal data is being used at any time and if unhappy about how their data is used may make a complaint.

6.1.9 Any person whose details (including photographs) are to be included on the Council's public website will be asked to give 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.

6.1.10 The Council will use exemptions under the DPA 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 section 29(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.

6.1.11 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.

7 Data Quality, Integrity and Retention

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

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

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

7.1.4 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.

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

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

7.1.7 Information will only be held for as long as is necessary after which the details will normally be deleted. 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.

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

8 Security

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

8.1.1 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.

8.1.2 An employee must only access personal data they need to use as part of their job. Inappropriate or unauthorised access may result in disciplinary action, including dismissal and criminal prosecution.

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

8.1.4 All data breaches (however minor) should be reported via the process detailed on the Information Governance intranet site.

8.1.5 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.

8.1.6 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.

8.1.7 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.

8.1.8 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.

8.1.9 Employees who process personal data out of the office (e.g. on site, on client premises, at home) can only do this with the express consent 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).

8.1.10 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.

8.1.11 Personal data will not be transferred outside the European Economic Area without the approval of the Head of ICT and Monitoring Officer.

9 Data Subjects Rights

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

9.1.2 The Council will provide individuals with a copy of the information held about them within 40 calendar days of receiving a request (subject access).

The maximum charge that can be made is £10, but the Council will not normally make a charge for this service.

9.1.3 On receiving a request for subject access the Council will check and require evidence of the identity of the individual and any further information required to isolate the records of that individual.

9.1.4 Where a subject access request has a broad scope, the Council may ask for more details from the data subject in order to locate the information that is of particular interest.

9.1.5 Where a large volume of information is held, the Council may seek to make the information available in ways other than providing a copy. This could include arranging an appointment for the data to be inspected within the Council.

9.1.6 In addition to the personal data itself, the individual will be provided with any supporting information that is needed to understand the data held, and the processing of it.

9.1.7 Where information located as part of a subject access request contains personal data about a third party, information will not be released unless the requirements set out in section 10.1 are met.

9.1.8 The introduction of the right of access to non-personal information held by the Council under the Freedom of Information Act 2000 may also need to be considered. This is because some requests may be for a combination of personal and non-personal information.

9.1.9 The Council has a Subject Access Form for Applicants and a Subject Access Procedure for Staff receiving requests to follow.

9.1.10 The Council will comply immediately with a request from an individual to cease sending them marketing or consultation information.

9.1.11 Requests from individuals to correct, rectify, block, or erase information that they regard as wrong information or to stop processing that is causing damage or distress will be considered by departments on a case by case basis. The individual concerned will be fully informed of the resulting decision and the reasons for it. Legal advice will be sort from the monitoring officer should a request not be supported by the department, or if considered sensitive/complex before coming to a decision.

9.1.12 An individual wishing to exercise any of their rights under the DPA should put their request in writing to the Council service which is processing their information.

9.1.13 All Subject Access requests received will be recorded on the Respond Database for monitoring and reporting purposes which is administered by the Complaints & FOI teams within each directorate.

10 Disclosure and Sharing

10.1 Third party access to information

10.1.1 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.

10.1.2 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

10.1.3 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.

10.1.4 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.

10.1.5 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.

10.1.6 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. However, without a Court Order there is no obligation on the Council to disclose the information.

10.1.7 Where the Council is not convinced that the third party has entitlement to the personal data, or that any exemptions under DPA apply, and that releasing information would breach the DP principles, the personal data will be withheld and only released on presentation of a Court Order.

10.2 Information sharing

10.2.1 Information sharing occurs when one or more agencies or professionals share information about a data subject for the better provision of a service or where it is in the best interests of that data subject.

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

10.2.3 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.

10.2.4 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.

10.2.5 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.

10.2.6 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 5.2, hereof.

10.2.7 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.

10.3 Contractual and partnership arrangements

10.3.1 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’.

10.3.2 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.

10.3.3 Where the parties are data controllers jointly or in common, the Council will liaise with the other party to ensure that all processing complies with DPA. The responsibilities of each data controller should be expressly and clearly laid out.

10.3.4 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 Legal Services as necessary.

10.3.5 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.

10.3.6 Any observed or suspected security incidents or security concerns should be reported to the Council.

10.3.7 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.

10.3.8 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.

11 Notification

11.1.1 The Council has a main corporate notification registered with the Information Commissioner under registration number Z5077191.

11.1.2 The Council will ensure that this notification is an accurate description of processing carried out by the Council. The Data & Information Group (DIG) will review the notification annually.

11.1.3 The Data Protection Officer is responsible for submitting this notification to the Information Commissioner.

11.1.4 When the Council plans to carry out new processing not covered by this notification, the manager responsible will inform the Data Protection Officer in good time to amend the notification (if necessary) within 28 days of processing beginning.

11.1.5 The Council also supports three further notifications 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).

11.1.6 Processing of personal data by Elected Members is covered by the Council's main corporate notification in respect of information held by the council.

11.1.7 Elected Members must maintain their own notification if they process personal data obtained by them for constituency or political purposes. Elected Members requiring their own notification must pay the relevant notification fee (currently £35) and must apply directly to Information Commissioner.

11.1.8 Failure to notify or maintaining an incomplete or inaccurate notification is a criminal offence.

12 Subject Access Requests and Data Protection Complaints

12.1.1 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.

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

Customer Relations
Chief Executive & Corporate Resources Department
PO Box 1953
Bristol BS37 0DB e-mail: CRSFeedback@southglos.gov.uk

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

Information Management Team
Department for Environment and Community Services
PO Box 1954
Bristol BS15 0DD e-mail: ECSFeedback@southglos.gov.uk

12.1.3 Complaints about the Council’s processing of personal data and rights under the Data Protection Act 1998 will be dealt with in accordance with this 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.

12.1.4 Unlike the Freedom of Information Act, the Data Protection Act does not set out a specific complaints regime for data protection issues. However individuals do have a right to request that the Information Commissioner make an assessment of compliance of particular circumstances with the DPA. If individuals are not happy about how we have handled their information they can contact the ICO via the following means:

This link to complete a short form which can then either be emailed to casework@ico.org.uk

Or sent to

Customer Contact
Information Commissioner's Office,
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire,
SK9 5AF

Alternatively visit their website - www.ico.gov.uk or contact them by phone on 03031231113

12.1.5 The Council will respond promptly and fully to any request for information about data protection compliance made by the Information Commissioner.

12.1.6 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 Legal Services for advice and support.

13 MONETARY PENALTIES (FINES)

The Information Commissioner has the power to fine organisations (and individuals) for serious breaches of the Data Protection Act. This is also called the power to issue a Monetary Penalty Notice. The Commissioner can require payment of a sum up to £500,000. Fines have been made against organisations that faxed sensitive personal data to the wrong recipients, lost a laptop that held personal data because of a burglary and lost unencrypted laptops that held personal data. 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.

14 Implementation

14.1.1 The responsibility for implementation of this policy rests with the Chief Executive, the Chief Officer's Management Team (COMT), the Senior Information Risk Officer, the Data & Information Group (DIG) and Monitoring Officer as the Data Protection Officer.

14.1.2 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.

14.1.3 On joining the Council, employees are required to undertake training on Data Protection and ICT 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.

14.1.4 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.

14.1.5 Supporting procedures for this policy have been created and are maintained within the Information Governance, 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.

14.1.6 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.

15 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. ICT 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. RIPA Communications Data Policy
13. Data Sharing Agreements, Protocols and Contracts (various)
14. National, Regional, Corporate and Departmental Policies and Procedures

16 Monitoring and Review

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

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

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

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