Data Protection Policy

May 2018

Document Control

Prepared By	Ann Wilson, Co-ordinator Registration, Records and Information, Regulatory Services
Authorised By	Leadership Panel
Source Location	
Published Location	
Other documents referenced	
Related documents	
Acknowledgements	
Classification	OFFICIAL

Document Revision

Version	Date Issued	Last Review Date	Author	Update Information
1.0				First draft issue
1.1	30/03/2016		Philomena Wilkes	Major revision
2.0	12/05/2016		Philomena Wilkes	Approved
2.1	04/05/2018		Ann Wilson	Major revision
3.0	24/05/2018		Ann Wilson	Approved
3.1	07/08/2018		Ann Wilson	Major revision

Policy Statement

The objective of data protection is to ensure that the rights and freedoms of data subjects are considered and protected in the collection and processing of personal data.

The purpose of this policy is to ensure that the personal data collected and processed by South Ayrshire Council ('the Council') is managed in accordance with the General Data Protection Regulation 2016 and the Data Protection Act 2018.

This policy applies to all staff and Elected Members of the Council. Other agencies and individuals working with the Council who have access to personal information held by the Council are also required to comply with this policy.

Contents

1. Introduction

The purpose of Data Protection law is to protect the personal data rights and privacy of living individuals. The Council is required to demonstrate to the Information Commissioner (UK Regulator of Data Protection law) that it is fully compliant with the General Data Protection Regulation 2016 (GDPR) and the Data Protection Act 2018 (DPA) both of which provide comprehensive protection of personal data.

The Council is required to demonstrate that it has incorporated the concept of 'Privacy by design' into its routine processes and procedures. The Council must also guarantee that it has adequate mechanisms in place to prevent against unauthorised or unlawful processing and accidental loss, damage or destruction of personal data.

In the course of its everyday business, the Council collects and processes personal information relating to South Ayrshire residents, current, past and prospective employees, suppliers, clients and others with whom it communicates. In addition, it may occasionally be required to collect and disseminate certain types of personal information to comply with the statutory requirements of government departments for business purposes. Given the operational importance and sensitivity of such data, it is essential that such information is managed and processed in an efficient and systematic manner to ensure the Council is not only compliant but can demonstrate its adherence to the six principles of GDPR (please see section 3 of this policy document).

To ensure best practice and full compliance with Data Protection law, the Council has established the Information Governance Team, based within Regulatory Services to advise and assist all services within the Council. The Service Lead – Democratic Governance is the named Data Protection Officer. The day to day responsibilities of the service lies with the Co-ordinator Registration, Records and Information. The Council is registered with the Information Commissioner as a data controller, registration number Z5548592

This policy will be reviewed bi-annually and may be altered at any time as appropriate.

2. Definitions

Personal Data

'Personal data' means any information relating to an identified or identifiable living person ('data subject' see below).

An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical,

physiological, genetic, mental, economic, cultural or social identity of that living person.

Data Subject

Data subject means ‘an individual who is the subject of personal data’. A data subject must be a living individual.

Data Controller

Data controller is defined as ‘a person (or organisation) who (either jointly or in common with other persons) determines the purposes for which, or the manner in which, any personal data are, or are to be, processed’.

Data Processor

The data processor means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Information Asset Register

An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and used efficiently to help the Council provide a service. Information assets have recognisable and manageable value, risk, content and lifecycles. Maintaining an Information Asset Register (IAR) is a requirement of the GDPR. The IAR is a simple way to help Council Officers understand and manage the Council’s information assets and the risks relating to those assets.

The Council’s IAR includes the following information:

- Identification of each information asset
- Where our information is held
- Why we keep it
- Who is allowed to access it
- How long we keep it

Processing

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

Special Category Data

This is personal data consisting of information relating to any of the following:

- Racial or ethnic origin.

- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Genetics.
- Biometrics (where used for ID purposes).
- Health.
- Sex life.
- Sexual orientation.

Special category personal data is subject to much stricter conditions of processing.

Personal data relating to criminal convictions and offences are not included within special category data per se but similar extra safeguards apply to its processing.

3. Principles of Data Protection

There are six data protection principles which the Council as the Data Controller is required to comply with. Personal data must be:

Principle 1 - Processed lawfully, fairly and in a transparent manner

The Council must have lawful authority for processing personal information and the purpose of the processing must be explained to the data subject. This links to the right of a data subject to be informed. This is achieved by providing data subjects with Privacy Notices (please see section 11 of this policy document). Any sharing of personal data with other organisations will be appropriately documented in the Privacy Notice.

Principle 2 – Obtained for specific, explicit and legitimate purposes

The Council must ensure that personal information is not processed for a purpose which is incompatible with the purpose for which it was collected. Processing must fall strictly within the purposes for which the data were obtained. Where the Council is obliged to obtain personal data for a statutory purpose, the data may not be processed for any other statutory purpose unless it directly relates to the original purpose.

It should be noted, further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

Principle 3 – Adequate, Relevant and limited to what is necessary

Personal information must be adequate relevant and limited to collecting only what is needed to get the job done given the purposes for which it is held. This will depend on circumstances, however care should be taken to ensure that information is not collected ‘just in

case' and that files are checked regularly to ensure that unnecessary information is removed.

Principle 4 – Accurate and where necessary kept up to date

Personal data must be accurate and up to date. Where it is discovered that information that is held by the Council is inaccurate, the error must be rectified immediately.

Principle 5 – Kept in a form that permits identification of data subjects and held for only as long as necessary

Personal data must be kept in a manner that allows data subjects to access it under a subject access request (please see section 10 of this policy document).Personal data must not be kept for longer than necessary for the purpose for which it was collected. The Council's Records Retention Schedule must be applied at all times.

Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures in order to safeguard the rights and freedoms of the data subject.

Principle 6 – Held securely

Appropriate security measures must be taken against unauthorised processing and against accidental loss, destruction, theft, or damage of personal data**.** Managers must therefore scrutinise their record keeping at all levels to ensure that appropriate security is in place.

If any information is processed on behalf of the Council by a third party, written contracts must be in place in terms of which the third party processor can act only on the Council's instructions and must comply in full with the security obligations which are imposed on the Council.

Where personal data has to be taken off-site, this will be restricted to only what is necessary to undertake the required task. The data must be kept secure at all times.

To help adhere to the above principles, the Council will ensure that:

i. all staff and Elected Members are aware of their specific responsibilities under the Data Protection law through policies and procedures which can be readily accessed via Rewired;

ii. services will be responsible for maintaining their entry in the Information Asset Register (IAR) to ensure it is accurate and kept up to date. Privacy Notices and any Data Protection Impact Assessments will be attached to the IAR as well as being shared with

Information Governance Department to be held in a central repository.

iii. services conduct a regular review and audit of the way personal information is managed and processed to ensure best practice and compliance with the law;

iv. staff managing and handling personal information receive appropriate training and supervision; and

v. all enquiries from data subjects requesting more information about how the Council handles their personal information are directed to the appropriate service and that any such enquiries are deal with promptly and courteously.

4. Processing special category data and criminal convictions

The DPA[1] requires data controllers who process special category (i.e. sensitive) personal data, or personal data relating to criminal convictions and offences to have an "appropriate policy document" in place setting out a number of additional safeguards for this data.

Please see appendix one for the Council's policy statement and additional safeguards on processing special category data and personal data relating to criminal convictions and offences.

5. Roles and Responsibilities

Overall responsibility and accountability for ensuring that all staff and associated third parties comply with data protection legislation, this Policy and associated policies and procedures, lies with the Head of Regulatory Services.

Information Asset Owners

The Information Asset Owners (IAOs) are the members of the Senior Management Team. Their role is to understand what information is held by their service, what is added and what is removed, how information is moved, and who has access and why. Through Service Leads and their teams, they must ensure that written procedures are in place and followed relating to these activities, risks are assessed, mitigated and the risk assessment processes are audited. They are also responsible for ensuring their service IAR entries are accurate and kept up to date.

Senior Information Risk Owner

The Senior Information Risk Owner (SIRO) has overall strategic responsibility for governance in relation to data protection risks. The SIRO:

- Acts as advocate for information risk at the Corporate Leadership Team.

[1] Data Protection Act 2018 Part 2, section 10

- Provides written advice to the Chief Finance Officer for the Annual Governance Statement relating to information risk.

- Drives culture change regarding information risks in a realistic and effective manner.

- Oversees the reporting and management of information incidents.

- In liaison with the Chief Executive and the Executive Directors, ensures the Information Asset Owner roles are in place to support the SIRO role.

The Council's SIRO is the Head of Regulatory Services.

Data Protection Officer

The role of the Data Protection Officer (DPO) is to:

- Inform and advise the Council and its employees about their obligations to comply with the General Data Protection Regulation and other data protection laws.

- Monitor compliance with the General Data Protection Regulation and other data protection laws, including the assignment of responsibilities, awareness raising and training of staff involved in the processing operations and related audits.

- Provide advice about data protection impact assessments and monitor their performance;

- Co-operate with the Information Commissioner's Office (ICO).

- Act as the contact point for the ICO's Office on issues related to the processing of personal data.

The Council's DPO is the Service Lead -Democratic Governance.

Co-ordinator Registration Records and Information

The Co-ordinator Registration Records and Information is responsible for developing, delivering and maintaining a comprehensive information governance and security framework for the Council. He/she will help ensure compliance with legislative frameworks governing the access to, retention, sharing and disposal of information.

He/she will collect information to identify the Council's processing activities, analyse the processing activities and provide information to the DPO so he/she can inform, advise and issue recommendations to the Council.

He/she will assist services in the carrying out of data protection impact assessments (DPIA), where required.

Senior ICT Security Analyst

The ICT Security Analyst is responsible for creating, implementing and maintaining the Council's security policy and procedures to reflect changing local and national requirements. This includes requirements arising from legislation, security standards and national guidance.

The ICT Security Analyst will support service areas on achieving best practice and compliance with security requirements.

Individual Members of Staff and Elected Members

Individual members of staff and elected members are responsible for protecting personal information held or processed on computer, or held in paper records, within their care.

They also have the responsibility to report any breach or potential breach immediately to the Information Governance Team/DPO (please see section 12 of this policy document).

6. Lawful basis for processing

The lawful basis for processing (using) personal data is set out in the GDPR. At least one of these must apply whenever the Council processes personal information:

- **Consent:** the data subject has given clear and unambiguous consent for the Council to process his/her personal data for a specific purpose.
- **Contract:** the processing is necessary for a contract that the Council has with the data subject, or because the data subject has asked the Council to take specific steps before entering into a contract.
- **Legal obligation**: the processing is necessary for the Council to comply with the law (not including contractual obligations).
- **Vital interests:** the processing is necessary to protect someone's life.
- **Public interest:** the processing is necessary for the Council to perform a task in the public interest or in the exercise of official authority vested in the Council.
- **Legitimate interests:** the processing is necessary for the purposes of legitimate interests pursued by the Council or a third party except where such interests are overridden by the interests of the data subject. This requires balancing the Council's interests against the individual's interests. However, this basis is not available to processing carried out by the Council in the performance of its official tasks

If the Council is processing special category data or criminal conviction data then they must consider the further conditions for processing. It is recommended that where processing involves special category or criminal data, advice is sought from the Co-ordinator Registration Records and Information.

7. Law Enforcement processing

Part three of the DPA transposes the EU Data Protection Directive 2016/680 (Law Enforcement Directive) into domestic UK law. The Directive complements the GDPR and sets out the requirements for the processing of personal data for 'law enforcement purposes' (LEP).

The Council processes personal data for LEP when carrying out processing in relation to offender management and when undertaking investigations and prosecuting offenders under Trading Standards and Environmental legislation.

The six law enforcement principles[2] are broadly the same as those in the GDPR, and are compatible across the two regimes. The Council adheres to the six law enforcement principles when processing personal data for law enforcement purposes only.

Data subjects rights [3] are similar to those found in the GDPR, however, the transparency requirements are not as strict, due to the potential to prejudice an ongoing investigation in certain circumstances.

The Council also has to be able to demonstrate overall compliance with all of the law enforcement principles.

Processing Sensitive Data

When processing sensitive data we must be able to demonstrate that the processing is strictly necessary and satisfies one of the conditions in Schedule 8 of the DPA or is based on consent. 'Strictly necessary' in this context means that the processing has to relate to a pressing social need, and we cannot reasonably achieve it through less intrusive means.

In this section, "sensitive processing"[4] means—
(a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
(b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;
(c) the processing of data concerning health;
(d) the processing of data concerning an individual's sex life or sexual orientation.

Part three of the DPA requires the Council to have the following safeguards in place for processing sensitive data. The Council must ensure that the processing:

- must be strictly necessary;
- must satisfy one of the conditions in Schedule 8; and
- there must be a policy document in place to demonstrate compliance, safeguards and processes.

[2] Data Protection Act 2018 Part 3, Chapter 2
[3] Data Protection Act 2018 Part 3, Chapter 3
[4] Data Protection Act 2018 Part 3, section 35 (8)

8. Exempting information from non-disclosure

The GDPR is designed to prevent access by third parties to a data subject's personal data. However, under the DPA[5] there are circumstances which allow disclosure of a data subject's personal data to a third party, or for it to be used in a situation that would normally be considered to breach the GDPR.

Exemptions from the non-disclosure of personal data are given below.

a) the prevention and detection of crime
b) the apprehension or prosecution of offenders
c) Taxation
d) Information required to be disclosed by law etc. or in connection with legal proceedings
e) Immigration

The Council will only use these exemptions where it is in the public interest to do so or where the functioning of the Council requires the processing of personal information to be exempt so that it can provide statutory services to members of the public.

9. Rights of Data Subjects

The GDPR provides data subjects with the following rights* regarding their personal information:

- The right to be informed about how their information will be used.
- The right of access to their personal information (subject access request)
- The right to rectification, which is the right to require the Council to correct any inaccuracies.
- The right to request the erasure of any personal information held by the Council where the Council no longer has a basis to hold the information.
- The right to request that the processing of their information is restricted.
- The right to data portability.
- The right to object to the Council processing their personal information.
- Rights in relation to automated decision making and profiling.

The Council will publish detailed information for the public that will set out what these rights are and how these can be exercised. Data subjects' rights are also contained in the Privacy Notices.

* Not all rights are absolute and will depend on the lawful basis on which the Council are relying to process the personal data.

10. Subject Access Requests

Data subjects have the right to request information that is held about them. The Council has a process for handling subject access requests, the relevant

[5] Data Protection Act 2018 Schedule 2, Part 1, Para 2

guidance can be found on Rewired. The public can access this information via the public website

The Council has 30 days to comply with a request and failure to meet this timescale may result in the ICO levying a fine.

11. Privacy Notices

Data subjects have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR. The Council must provide data subjects with information including: the Council's purposes for processing their personal data, the Council's retention periods for that personal data, and with whom it will be shared, within a 'Privacy Notice'.

Privacy Notices must be concise, transparent, intelligible, easily accessible, and must use clear and plain language.

The Information Governance Department will monitor and police the use of Privacy Notices to ensure that they are regularly reviewed, and where necessary, updated.

12. Breaches

Organisations which process personal data must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of, or damage to, personal data. Despite the security measures taken to protect personal data held by the Council, a breach may occur.

The Council has a legal requirement to notify the ICO within **72 hours** of any personal data breach where it is likely to result in a risk to the rights and freedoms of data subjects. Failure to notify the ICO may result in a significant fine being imposed.

It is the DPO's responsibility to assess each personal data breach for consideration to report to the ICO and also has a duty to report any personal data breach to any affected data subjects. Therefore it is imperative all personal data breaches, both suspected, and confirmed, are reported immediately to the Information Governance Team/DPO:

By emailing – DataProtection@south-ayrshire.gov.uk
And putting 'Data **breach'** in the subject heading of the email and attaching the data breach electronic reporting form.

Staff who have no PC access should report a data protection breach to their line manager in the first instance and in the event that this is not practical, they will be expected to phone the Information Governance Team:

By calling – 01292 612223.

Contract owners must take steps to remind contractors and third party users of Council information systems of:

- their legal obligation to report personal data breaches as per the GDPR
- their contractual obligations, where applicable
- in all other cases; encourage support of good practice, as outlined above.

Contract owners must ensure that when contracts are negotiated or renewed they contain appropriate obligations to support this procedure. Support is available from the Council's procurement and legal teams.

Where an incident involves the loss of ICT equipment or functionality, the event should also be logged on the ICT Helpdesk:

By emailing ICTServiceDesk@south-ayrshire.gov.uk
By telephoning - 01292 612406
By accessing the form on Rewired

13. Notification

The Council must advise the Information Commissioner's Office that it holds personal information about living people. It must also pay a fee in accordance with the Data Protection (Charges and Information) Regulations 2018.

14. Data sharing

All sharing of data with other organisations must be appropriately documented and a Data Sharing Agreement in place before any data is shared.

15. Related policies and Procedures

South Ayrshire Council's Records Management Policy.
South Ayrshire Council's Information Security Policy.
South Ayrshire Council's Records Retention Schedule.
South Ayrshire Council's Freedom of Information Policy.

16. Further Information and Guidance

The Co-ordinator Registration Records and Information
Regulatory Services
South Ayrshire Council
County Buildings
Wellington Square
Ayr
KA7 1DR
E-mail: dataprotection@south-ayrhsire.gov.uk
Tel: 01292 612223

Further information is also available from the Information Commissioner's website

Appendix 1

Policy statement and additional safeguards on processing special category data and personal data relating to criminal convictions and offences

Policy Statement

1: Lawfulness, fairness and transparency:
The Council will determine and document the legal basis under which the data is processed. The Council will also have a valid legal basis for disclosing this personal data to third parties where it is appropriate to do so, Privacy notices in-line with the GDPR requirements are available, please see https://www.south-ayrshire.gov.uk/privacy-notices/ for further details. We are presently updating our data processor agreements and data sharing agreements to reflect the new legal requirements.

2: Purpose limitation:
The Council has clearly set out the purposes for which data are collected in the relevant privacy statements. This includes reference to further use of data for internal management information purposes. A limited set of data is required for research and archiving purposes; the Council has put in place appropriate safeguards for these activities as required by Article 89 of the GDPR.

3: Data minimisation:
The Council will only collect the personal information we need to provide you with relevant information, services and support. The Council is continually assessing the data captured by its services and takes every opportunity to critically assess the need for collecting specific personal data. If we identify areas where unnecessary personal data is being captured, we will cease to collect and capture this specific personal data.

4: Accuracy:
The Council is continually checking data for accuracy and, where any inaccuracies are discovered, they are promptly corrected and any third party recipients of the inaccurate data notified of the correction.

5: Storage limitation:
The Council retain personal data for no longer than reasonably necessary. Sometimes this time period is set out in law, but in most cases it is based on business need. We maintain a records retention and disposal schedule which sets out how long we hold different types of information, you can view this on our website at https://www.south-ayrshire.gov.uk/foi/policy.aspx . Ayrshire Archives materials are held subject to appropriate safeguards in terms of Article 89 of the GDPR.
Ongoing management of the council's records and information is subject to the provisions of our Records Management Plan, which was developed in terms of the Public Records (Scotland) Act 2011 and approved by the Keeper of the Records of Scotland. It is available online at https://www.south-ayrshire.gov.uk/foi/policy.aspx. The Records Management Plan sets out, in much greater detail, the provisions under which the Council complies with its obligations under public records legislation, data protection and information security and is complementary to this policy statement.

6: Integrity and confidentiality:
The Council has an approved Information Security Policy which sets out roles and responsibilities within the organisation in relation to information security. All staff are required to complete and pass information security training and be conversant in our ICT policies and procedures in relation to acceptable use of IT facilities. Our ICT systems have appropriate protective measures and the systems are subject to external

assessment and validation. We have policies and procedures in place to reduce the information security risks arising from use of hard copy documentation.

The Council is also required to have additional safeguards by maintaining this policy statement, reviewing and updating it (if appropriate) and making it available to the ICO on request.

The Council is also required to maintain an information asset register as per Article 30 of the GDPR.