Information Governance

Data Protection Policy

September 2023

Document Control

Prepared By	Deborah McVey, Co-ordinator Registration, Records and Information, Democratic Governance, Chief Executive's Office
Authorised By	2023: Cationa Caves, Head of Legal & Regulatory Services (under delegate powers) 2018: South Ayrshire Council's Leadership Panel
Published Location	Data protection - South Ayrshire Council (south-ayrshire.gov.uk)
Classification	OFFICIAL

Document Revision

Version	Date Issued	Last Review Date	Author	Update Information
3.0	24/05/2018		Ann Wilson	Approved
3.1	01/09/2023	01/09/2024	Deborah McVey	Minor Amendments to reflect legislation changes

Policy Statement

The objective of data protection is to ensure that the rights and freedoms of data subjects are considered 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 UK Data Protection Regulation ("UK GDPR") read in conjunction with the Data Protection Act 2018 ("DPA 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 we are fully compliant with the UK GDPR as supplemented by the DPA 2018 and have incorporated the concept of 'Privacy by Design' into our routine processes and procedures. The Council must also guarantee that we have adequate mechanisms in place to prevent against unauthorised or unlawful processing and accidental loss, damage, or destruction of personal data.

During our 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 we communicate. In addition, we 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 our adherence to the six principles of UK 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 responsibility of the service lies with the Co-ordinator Registration, Records, and Information. The Council is registered with the Information Commissioner as a data controller.

This policy will be reviewed 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, 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 (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 UK GDPR. The IAR is a simple way to help Council Officers understand and manage the Council’s information assets and the risks around 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.
- How the information gets in and out of the Council

Processing

The definition of processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether 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, but similar extra safeguards also 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 8 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 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 manner that allows data subjects to access it under a subject access request (please see Section 7 of this Policy document). Personal data must not be kept for longer than necessary for the purpose it was collected. The Council's Records Retention Schedule must be always applied. Records management - South Ayrshire Council (south-ayrshire.gov.uk)

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 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 must be taken off-site, this will be restricted to only what is necessary to undertake the required task. The data must be always kept secure.

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 the Core;

ii. Services will be responsible to maintain 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 Assessment will be linked to or 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 wanting more information about how the Council handles our personal information are directed to the appropriate service and that any such enquiries are deal with promptly and courteously.

4. 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 Council's Senior Management Team

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 Senior Management Team.
- 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 Legal & Regulatory Services.

Data Protection Officer

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

- Inform and advise the Council and our employees about their obligations to comply with the General Data Protection Regulation and other data protection laws.
- Monitor compliance with the UK GDPR 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. They will help ensure compliance with legislative frameworks governing the access to, retention, sharing and disposal of information.

They will collect information to identify the Council's processing activities, analyse the processing activities and provide information to the DPO to inform, advise and issue recommendations to the Council.

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

Information Security Officer

The Information Security Officer 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 Information Security Officer 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 9 of this policy document).

5. Lawful basis for processing

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

Consent

The data subject has given clear consent for the Council to process their 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 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 unless there is a good reason to protect the data subject's personal data which overrides those legitimate interests. However, this basis is not available to processing carried out by the Council in the performance of its official tasks: it can only apply to the Council when it is fulfilling a different role.

If the Council is processing special category data or criminal conviction data, then we must consider the further conditions for processing. It is recommended that in the case when processing involves special category or criminal data, advice is sought from the Co-ordinator Registration Records and Information at dataprotection@south-ayrshire.gov.uk.

6. 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.

7. Subject Access Requests

Data subjects have the right to request information which is held about themselves. The Council has a process for handling subject access requests, the relevant guidance can be found on the Core. The public can access this information via the public website.

The Council has one calendar month to comply with a request, unless the request is of a complex nature and with prior approval of the Co-ordinator of Registration, Records & Information. Failure to meet this timescale may result in the ICO levying a fine.

8. 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 UK GDPR. The Council must provide data subjects with information including: our purposes for processing their personal data, our 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 it must use clear and plain language. To meet this requirement the Council will adopt a combination of different techniques including layering, dashboards, and just-in-time notices to inform our residents on how we use their personal data.

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

9. 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. The DPO 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 if 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 UK 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 the Core

10. 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.

11. Data sharing

The Act does not prohibit the sharing of personal data where it is appropriate. All sharing of data with other organisations must be appropriately documented and a Data Sharing Agreement in place before any data is shared.

12. 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.**

13. Further Information and Guidance

The Co-ordinator Registration Records and Information
Chief Executive's Office
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