



Data Protection Policy

2025

Date	Version	Owner	Comments
30/11/20	0.1	Head of Legal and Regulatory Support	
December 2020	1.0	Head of Legal and Regulatory Support	Version approved by SMT
October 2025	1.1		

1.0 Introduction and Policy Statement

- 1.1 Argyll and Bute Council ('the Council') collects and processes personal information about its customers, employees and others to allow the Council to carry out many of its functions and responsibilities. This personal information, however, it is acquired, held, processed, released or destroyed, must be dealt with lawfully and appropriately in accordance with Data Protection Legislation.
- 1.2 Dealing appropriately with personal information will not only ensure that the Council complies with its legal obligations but will contribute to maintaining the confidence of customers, employees and others.
- 1.3 This Policy sets out the Council's commitment to ensuring that any Personal Data, including Special Category Personal Data, is processed in compliance with Data Protection Legislation. The Council seeks to ensure that good data protection practice is embedded in the culture of the Council and its employees.
- 1.4 This Policy sets out appropriate guidance and safeguards to ensure compliance with Data Protection Legislation.
- 1.5 The Council will ensure that all employees who handle Personal Data on its behalf are made aware of their responsibilities under this Policy and other relevant data protection and information security policies and that adequate training and supervision is provided.
- 1.6 To comply with Data Protection Legislation, information about individuals must be:
 - collected lawfully;
 - used fairly;
 - accurate and kept up to date;
 - stored safely and securely;
 - retained no longer than is necessary and;
 - not disclosed to any third party unlawfully.

The Council will inform individuals about the processing that it undertakes, through privacy notices and direct contact, and will make it clear to individuals what is happening with and to their Personal Data.

2.0 Definitions

- 2.1 The table below outlines key definitions that are referred to within this Policy and Data Protection Legislation

Personal Data – Any information relating to an identified or identifiable living natural person (data subject); an identifiable person is one who can be identified, directly or indirectly. In particular, by reference to an identification number or more factors specified to his physical, physiological, mental, economic, cultural or social identity.

Special Category Personal Data - this is Personal Data consisting of information relating to any of the following:

- Racial or ethnic origin.

- Political opinions.
- Religious or philosophical beliefs.
- Trades Union membership.
- Genetics.
- Biometrics (where used for ID purposes).
- Health.
- Sex Life.
- Sexual Orientation.

Record - A record is recorded information, in any form, including data in systems created, received and maintained by the Council and kept as evidence of such activity.

Subject Access Request - This is a right of access by individuals to their Personal Data held by the Council.

Records Management - The control of the Council records during their lifetime, from creation to storage until archiving or destruction.

Processing - The definition of Processing covers everything from obtaining and gathering in information to using the information and, eventually, destroying the information.

Data Controller - A Data Controller is a person or organisation who decides how any personal information can be held and processed, and for what purposes. The Council is a Data Controller and individual Elected Members can be Data Controllers.

Data Processor - This role is carried by any person other than a Council employee (for example, contractors and agents) who process personal information on behalf of the Council.

Data Protection Legislation - the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

3.0 Scope

- 3.1 This Policy applies to all employees and Elected Members of the Council. Any breach of Data Protection Legislation or this Policy may result in disciplinary action for an employee, referral of an Elected Member to the Standards Commission and may also constitute a criminal offence.
- 3.2 Other third parties, including but not limited to, agencies, consultants, contractors, volunteers, agents or any other individual Processing Personal Data on behalf of the Council, are required to comply with this Policy.
- 3.3 This Policy applies to all situations where the Council processes (collects, stores, uses, shares) Personal Data about living individuals. It includes information stored in any format including but not limited to Personal Data held electronically, on paper, on CCTV, in photographs and on audio equipment.

4.0 Responsibilities

- 4.1 The Council is the Data Controller under Data Protection Legislation.

- 4.2 The Strategic Management Team, Chief Officers and Service Managers are responsible for ensuring their teams and employees are aware of this Policy and for developing and encouraging robust information handling practices.
- 4.3 Compliance with Data Protection Legislation is the responsibility of all employees and Elected Members who process personal information.
- 4.4 Each Service and its senior management will retain a service responsibility for compliance with the provisions of the Data Protection Legislation and this Policy.
- 4.5 All employees will be responsible for following procedures and systems for maintaining appropriate security of the Personal Data to which they have access.
- 4.6 The Strategic Management Team will ensure that employees are provided with guidance, training and procedures to promote a culture of compliance with the Data Protection Legislation and with this Policy.
- 4.7 The Council's Senior Information Risk Owner (SIRO) sits on the Strategic Management Team and has overall responsibility for Information Management and Information Risk Management within the Council.

The SIRO:

- Acts as an advocate for information risk at the Strategic Management Team;
 - Drives culture change regarding information risks in a realistic and effective manner;
 - Is consulted on matters arising from information incidents; and
 - In liaison with the Chief Executive and other Executive Directors, ensures the Information Asset Owner and supporting roles within Services are in place to support the SIRO role.
- 4.8 The Council's Data Protection Officer (DPO) has corporate responsibility to:
 - Inform and advise the Council and its employees about their obligations to comply with the Data Protection Legislation and other data protection laws;
 - Monitor compliance with Data Protection Legislation and other data protection laws, including the assignment of responsibilities, raising awareness, developing training, training employees involved in the Processing areas and working on audit related matters;
 - Provide advice about Data Protection Impact Assessments (explained further in section 12) and monitor their performance;
 - Co-operate with the supervisory authority (the Information Commissioner's Office); and
 - Act as a point of contact for the Information Commissioner's Office on issues related to the Processing of Personal Data.

The Council's DPO is Iain Jackson, Governance, Risk and Safety Manager, Kilmory, Lochgilphead, Argyll and can be contacted at data.protection@argyll-bute.gov.uk

5.0 Personal/Special Category Data

- 5.1 The Council processes both personal and Special Category Data of employees, service users and third parties as is necessary to carry out its many functions and responsibilities.

Processing conditions – Personal data

- Consent of the data subject
- Contractual necessity
- Legal obligation of the controller
- Vital interests of the individual
- Performance of a task in the public interest or in the exercise of official authority
- Legitimate interest of the controller or the third party

Special Category Personal Data is subject to much stricter conditions of Processing:

- Explicit consent of the data subject
- Compliance with employment, social security and social protection law obligations
- Vital interests of the data subject
- Processing by a not-for-profit body
- Personal data manifestly made public by the data subject
- Establishing, exercising or defending legal claims or whenever courts are acting in their judicial capacity
- Substantial public interest
- Provision of medical or social care or treatment
- Public interest in the area of public health
- Archiving in the public interest, scientific or historical research or statistical purposes

6.0 Data Protection Principles

6.1 The Principles

The Council handles all personal data in line with the seven data protection principles set out in Article 5 of the UK GDPR.

1. Lawfulness, fairness and transparency
We identify and record a valid lawful basis for each processing activity, treat people fairly, and explain clearly what we do with their data through privacy notices.
2. Purpose limitation
We collect personal data for specified, explicit and legitimate purposes and do not use it in ways that are incompatible with those purposes. Where data is kept for archiving, research or statistics, we apply Article 89(1) safeguards.
3. Data minimisation
We collect and keep only the data that is adequate, relevant and limited to what is necessary.
4. Accuracy
We keep personal data accurate and up to date and take reasonable steps to correct or delete inaccuracies without delay.
5. Storage limitation
We do not keep identifiable personal data longer than necessary for the purposes collected, applying documented retention rules; extended retention for archiving/research/statistics is supported by Article 89(1) safeguards.

6. Integrity and confidentiality (security)

We protect personal data with appropriate technical and organisational measures to ensure confidentiality, integrity and availability.

7. Accountability

We are responsible for, and are able to demonstrate, compliance with these principles.

6.2 Applying the principles in practice

To apply these principles in practice, the Council:

a) Records lawful bases in the Information Asset Register (IAR) and ensures all processing reflects the recorded basis.

b) Documents data sharing with other organisations, including the legal basis and safeguards.

c) Provides clear privacy information at or before collection, tailored to audience and context.

d) Applies data minimisation by collecting the minimum necessary information and periodically reviewing fields.

e) Maintains accuracy through defined update/correction processes and prompt propagation of corrections to recipients.

f) Follows retention schedules for storage limitation and secure disposal, with Article 89(1) safeguards where applicable.

g) Enables data subject rights via documented procedures and service standards.

h) Protects data security with proportionate controls (policy, access, training, technical safeguards, monitoring).

i) Prevents loss or unauthorised disclosure through risk assessment, incident response and continuous improvement.

j) Controls off-site processing by applying equivalent safeguards when data is accessed or transported outside Council premises.

7.0 Data Subject Rights

7.1 Data Subjects have the following rights regarding data Processing and the data that is recorded about them:

- Right to be informed;
- Right of access;
- Right to rectification of inaccurate data;
- Right to erasure in certain circumstances;
- Right to object to certain Processing, including the right to prevent Processing for direct marketing;
- Right to prevent automated decision-making;
- Right to data portability; and
- Right to claim compensation for damages caused by a data breach.

- 7.2 The Council will ensure that the rights of Data Subjects are respected. Advice can be sought by contacting the Compliance and Regulatory Team by email: dataprotection@argyll-bute.gov.uk

8.0 Data Protection Registration

- 8.1 The Data Protection (Charges and Information) Regulations 2018 requires organisations that process personal information to pay a fee to the Information Commissioner's Office (ICO), unless exempt. The Information Commissioner maintains a public register of notified Data Controllers. Payment of the data protection fee on behalf of the Council is the responsibility of the Head of Legal and Regulatory Support. The Council is registered under Z5909574, and the Licensing Board is registered under ZA171116.
- 8.2 Individual Elected Members are exempt by law from payment of the data protection fee.

9.0 Documentation of Processing Activities

- 9.1 There is a legal requirement to document Processing activities under the Data Protection Legislation. All Council Departments have an Information Asset Register (IAR) which incorporates the basis of the Council's documentation of processing activities. It is the responsibility of each Service to update the IAR and ensure that the information relevant to their Service is accurate at all times.

10.0 Contracts

- 10.1 Where an organisation processes Personal Data on behalf of the Council there must be a contract in place that contains the Council's Terms and Conditions, which includes the Council's standard data protection clauses.

11.0 Data Sharing

- 11.1 Data sharing takes place when Personal Data is shared with another organisation for its own purposes. This is separate from when the organisation is processing the Personal Data on behalf of the Council.
- 11.2 An appropriate written agreement for the sharing of Personal Data (known as a Data Sharing Agreement or an Information Sharing Protocol) must be in place before any systematic or large-scale Personal Data sharing takes place. Legal and Regulatory Support must be consulted prior to any such agreement being made.
- 11.3 Completed Data Sharing Agreements should be sent to dataprotection@argyll-bute.gov.uk A register of completed Data Sharing Agreements and Information Sharing Protocols is maintained by Legal and Regulatory Support.

12.0 Data Protection Impact Assessments

- 12.1 A Data Protection Impact Assessment (DPIA) will be undertaken to identify and minimise the privacy risks of any new project that will involve Processing Personal Data or where processing is being undertaken in a different way. The lead officer for the project or policy will be responsible for ensuring that the DPIA is undertaken. The DPO will assist Services to

identify the need for a DPIA, provide guidance for the assessment process, and make recommendations to ensure the Council's compliance with the Data Protection Legislation.

- 12.2 Completed DPIAs should be sent to dataprotection@argyll-bute.gov.uk A register of completed DPIAs is maintained by Legal and Regulatory Support.

13.0 Data Breaches

- 13.1 The Council has a legal responsibility to ensure that Personal Data is processed securely, held confidentially and with integrity and accessed by only those who have a justified right of access. Despite the security measures taken to protect Personal Data held by the Council, a breach can happen.
- 13.2 The Council has a Data Breach Notification Protocol which is to be followed in the event of a data breach.
- 13.3 It is a criminal offence under Data Protection Legislation to knowingly or recklessly obtain, disclose or procure Personal Data without the consent of the Data Controller and the Council reserves the right to report any such incidences to the Information Commissioner's Office and/or Police Scotland.

14.0 Governance

- 14.1 The Policy & Resources Committee will act as the final forum for the consideration of any matters related to Data Protection Legislation and Policy. This Policy will be reviewed at least every 3 years.

15.0 Conclusion

- 15.1 The Council subscribes to the principles of the Data Protection Legislation and will continue to develop policies, procedures and guidelines to ensure compliance with its legal obligations.