Comhairle Aonghais

ANGUS COUNCIL

DATA PROTECTION POLICY

Version:	V01.1
Author:	Angela Dunlop, Team Leader Information Governance
Owner:	Jackie Buchanan – Chief Information Governance Officer
Date of Approval:	April 2020
Approved by:	Information Governance Working Group
Date issued:	April 2020
Review Period	Biennial
Next review date:	April 2025

Amendment Form

Version	Date	Brief Summary of Changes	Author
01	07 April 2020	Brief Changes	Angela Dunlop
01.1	25 October 2021	Brief Changes	Angela Dunlop
01.2	12 April 2022	Brief Changes	Angela Dunlop
01.2	19 April 2023	Links checked no changes	Claire McBean
01.3	21 February 2024	Brief Changes	Claire McBean

Contents

Policy Statement

To operate efficiently, Angus Council must collect and use information about people with whom it works. These may include members of the public, current, past and prospective employees, clients and customers, and suppliers. In addition, it may be required by law to collect and use information to comply with the requirements of government.

Angus Council regards respect for the privacy of individuals and the lawful and careful treatment of personal information as very important to its successful operations and to maintaining confidence between the council and those with whom it carries out business. The council will ensure that it treats personal information lawfully and proportionately.

To this end Angus Council is committed to protecting the rights and privacy of individuals including those rights set out in the General Data Protection Regulation (GDPR); the Data Protection Act 2018 (DPA) and other data protection legislation.

The council's principal aim is to ensure that all personal data processing carried out by the council, or on its behalf, complies with the six data protection principles and other key legislative requirements.

This policy applies to all employees and elected members as well as consultants, volunteers, contractors, agents or any other individual performing a function on behalf of the council.

1. Introduction

The council increasingly depends on computer systems and paper records (paper files) to carry out much of its normal business. In 1998, when the previous Data Protection Act 1998 was enacted by Parliament, the internet was in its infancy, social media and smart telephones had not been invented and the way we shared information was very different. The GDPR and DPA protect the rights of individuals in these new circumstances. This policy sets out how the council will protect the rights of individuals and comply with the law.

To comply with the current legislation, all employees, elected members, consultants, volunteers, contractors and other agents of the council who use its computer facilities or paper files to hold and process personal information must comply with the policy.

2. Definitions

Personal Data

This is data which relates to a living individual ("data subject") who can be identified:

- From the data; or
- 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 the name, address, telephone number, national insurance number as well as any 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. Under GDPR, IP addresses are also included as personal data.

Special Category Data

This is personal data consisting of information as 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.

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.

Vital Record

This is a record without which an organisation would be unable to function or to prove that a key activity had taken place.

Format

A record can be in any format including (but not limited to) paper files, e-mail, audio/visual, electronic documents, systems data, databases, digital images and photographs.

Records Management

The control of the council records during their lifetime, from creation to storage until archiving or destruction.

Record Keeping System

A system or procedure by which the records of the council are created, captured, secured, maintained and disposed.

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. Angus Council is a Data Controller.

Joint Data Controllers

These are people or organisations (for example, Angus Council, NHS Tayside or Police Scotland) who jointly process and share information.

Data Processor

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

Data Protection Impact Assessments – *previously known as Privacy Impact Assessment*

Data Protection Impact Assessments (DPIAs) are a tool that you can use to identify and reduce the privacy risks of your projects. A DPIA can reduce the risks of harm to individuals through the misuse of their personal information. A DPIA can also help you to design more efficient and effective processes for handling personal data. There is a DPIA Template available for staff to use and a central record held of all agreed DPIAs.

Privacy Notices

A privacy notice is a statement that describes how Angus Council will collect, use, retain and disclose personal information.

Angus Council has a two-tiered effect

- **Privacy Notice A – a service specific notice to be created by services**
- **Privacy Notice B –** a full comprehensive notice
-

3. Roles and Responsibilities

Chief Information Governance Officer

The Chief Information Governance Officer (CIGO) has overall strategic responsibility for governance in relation to data protection risks. The council's CIGO is the Director of Legal, Governance and Change. The CIGO:

- Acts as advocate for information risk at the Council Leadership Team (CLT).
- Drives culture change regarding information risks in a realistic and effective manner.
- Oversees the reporting and management of information incidents.

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 GDPR and other data protection laws.
- Monitor compliance with the 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 supervisory authority (the Information Commissioner's Office).
- Act as the contact point for the Information Commissioner's Office on issues related to the processing of personal data.

The Council's DPO is the Service Leader – Legal and Procurement.

Team Leader - Information Governance

The Team Leader – Information Governance will lead the development and implementation of information governance across the council and contribute to emerging digital processes for storage and retrieval of information.

The Team Leader – Information Governance will oversee the council's compliance with regulatory and statutory provisions insofar as they apply to records management.

The Team Leader – Information Governance will oversee the co-ordination of council responses to information requests and ensure compliance with freedom of information, data protection and associated legislation as appropriate.

Information Technology Security

The Team Leader Network and Security in IT will support service areas on achieving best practice and compliance with security requirements.

Archivist

The Archivist will ensure that policies and procedures are compatible with legislation, particularly in relation to the transfer of records to the archive and their subsequent storage and access.

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.

Senior Information Officers

The Senior Information Officers (SIOs) are the members of the Information Governance Steering Group (IGSG). Their role is to:

- To give strategic direction, leadership and support to the Information Governance Working Group (IGWG)
- To ensure compliance with the Information Governance Strategy and Information Governance Management Framework
- Strategic decision making, in relation to information governance policies and procedures
- Stakeholder communications
- Conflict resolution
- Identify and monitor risk

Information Officers

Each SIO has nominated one or more Information Officer(s) IO(s) to the council's IGWG. They are responsible for providing routine advice on data protection to their respective services.

- To assist with the implementation of all information policies at a service level;
- To assist with the maintenance and revision of retention and disposal schedules at a service level;
- To develop and maintain the service Information Asset Register
- To process data protection and freedom of information requests at a service level;
- To monitor the implementation of the information governance training programme at a service level;
- To communicate best practice, guidance and information at a service level

Information Governance Steering Group

The IGSG is led by the council's CIGO and accountable to CLT. The IGSG is responsible for effective information management and governance.

The agreed terms of reference are:

- To develop and monitor implementation of the council's Information Governance Strategy and associated improvement plans;
- To raise awareness of the council's Information Governance Management Framework;
- To identify and monitor information risk;
- To oversee performance indicators for the council's information handling activities to ensure compliance with legislation;
- To direct and support the work of the IGWG and directorate working groups; and
- To provide regular reports to the CLT.

Information Governance Working Group

The IGWG is responsible for the day-to-day implementation and monitoring of information governance policies and procedures and for promoting information governance best practice across the organisation.

The agreed terms of reference are:

- To communicate/cascade best practice, guidance and information at a service level;
- To regularly review, update, approve (minor changes) and implement the council's information governance policies;
- To implement relevant actions identified in the Information Governance Improvement Plan or any other associated improvement plans;
- To assist with annual Progress Update Reviews for approval by the National Records of Scotland in connection with the council's Records Management Plan; and
- To provide a focal point for the resolution and/or discussion of all information governance issues.

4. Lawful Bases for Processing Personal Information

The lawful bases for processing are set out in the GDPR. At least one of these must apply whenever the council processes personal information:

- **Consent:** the individual has given clear 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 individual, or because the individual 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 unless there is a good reason to protect the individual'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.

5. Rights of Individuals

The GDPR provides individuals 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.
- 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.

There is more information in our privacy notices and our full privacy notice statement which can be found on the Information Governance website.

6. The Data Protection Principles

The GDPR sets out six main principles for the processing of personal information which are legally binding on the council. The personal information must be:

1. Processed lawfully, fairly and in a transparent manner in relation to the data subject.

2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

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

5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject.

6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

7. Notifying the Information Commissioner

The council must advise the Information Commissioner's Office that it holds personal information about living people.

8. Processing Personal Information

Each service has completed an Information Asset Register (IAR) and this is our record of the information we collect, what we do with it and how long we store it for

The council will hold and process personal information only to support those activities it is legally entitled to carry out.

The council may on occasion share personal information with other organisations. In doing so, the council will comply with the provisions of the Information Commissioner's Data Sharing Code of Practice and enter into a data sharing agreement if appropriate. A register is kept centrally of all our data sharing agreements.

The person the personal information is collected from must be advised of the purpose for which the information will be held or processed and who the information may be shared with. There is more information of our data sharing agreements, privacy notices and our full privacy statement on the Information Governance website.

9. Training

All staff will be provided with training in basic data protection law and practice as soon as reasonably practicable after starting to work for the council. Thereafter staff will be required to complete the data protection elearning on an annual basis. Agency workers and students are required to sign a Third Party Agreement.

Any new IOs will be trained in data protection relating to their responsibilities for their business area.

Managers may wish to request in-depth training for their staff, particularly if they are dealing with Special Category Data. In these circumstances they should contact the relevant IO in the first instance to enable appropriate arrangements to be made.

Elected Members will be provided with training in basic data protection law and practice as soon as reasonably practicable after they are elected as part of the induction programme.

10. Information Security

The council's approach to Information Security is set out in its Information Security Policy and its Information Technology (IT) Security Policy.

11. Complaints

Any complaints received by, or on behalf of, a member of the public containing allegations of inappropriate disclosure of information will be dealt with in the normal way through the council's Complaints Handling Procedure in the first instance. In addition it may be dealt with in accordance with the Data Protection Breach Response Plan.

If an individual does not feel that the council is treating their data appropriately or has not answered their complaint they can contact the Information Commissioner.

12. Breaches of Security

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 can happen.

If a breach occurs an IO within the directorate must immediately be informed who will contact the council's Data Protection Officer in accordance with the Data Protection Breach Response Plan.

13. Monitoring and Reporting

This policy will be reviewed biennially by the Team Leader - Information Governance.

Proposed changes to information governance policies or procedures will be considered by the IGWG in the first instance.

A review of the council's compliance with data protection legislation and best practice will be reported regularly to the IGSG.

14. Related Policies and Procedures

- Angus Council Records Management Policy.
- Information Security Policy.
- Information Technology (IT) Security Policy.

15. Further Information and Guidance

Data Protection Officer
Service Leader (Legal and Procurement)
Legal, Governance and Change
Angus House
Orchardbank Business Park
Forfar
DD8 1AN

E-mail: InformationGovernance@angus.gov.uk
Further information is also available from the Information Commissioner's website