Dumfries and Galloway Council

Data Protection Policy

Dumfries & Galloway COUNCIL

Contents

1. Policy Statement

To operate efficiently, Dumfries and Galloway 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.

Dumfries and Galloway 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 Dumfries and Galloway Council is committed to protecting the rights and privacy of individuals including those rights set out in the General Data Protection Regulation 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.

2. 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 General Data Protection Regulation protects 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.

3. Definitions

3.1 Personal Data

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

- From the data.
- 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.

3.2 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.

3.3 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.

3.4 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.

3.5 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.

3.6 Records Management

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

3.7 Record Keeping System

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

3.8 Processing

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

3.9 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. Dumfries and Galloway Council is a Data Controller.

3.10 Joint Data Controllers

These are people or organisations (for example, NHS Dumfries and Galloway) who jointly process and share information.

3.11 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.

4. Roles and Responsibilities

4.1 All Staff and Elected Members

Data Protection is everybody's responsibility and is something that should be considered as part of normal everyday working practice. It is the responsibility of all Council staff and Elected Members to manage records and information in line with the relevant policies and procedures.

4.2 Senior Information Risk Officer

The Director, Corporate Services, is the Council's Senior Information Risk Officer.

4.3 Data Protection Officer

GDPR requires the Council to have a Data Protection Officer (DPO). At present, this role is undertaken by the Democratic Services Manager. The DPO provides advice and guidance on GDPR; monitors the organisation's compliance and is the main point of contact for the Information Commissioner's Office.

4.4 Records and Information Management Officer

Day-to-day responsibility for the implementation and operation of records management, including responsibility for producing and implementing records management policies and procedures and providing the necessary advice and guidance to Council services.

4.5 Council Archivist

Responsible for the receipt and management of all archival records held or to be held by the Council.

4.6 Policy and Resources Committee

Responsible for the consideration and approval of the associated strategies and policies.

4.7 Business Management Group

Records management progress is reported to the Business Management Group. Directorate Business Managers are expected to lead on records management for their Directorate and report back. Business Managers are also responsible for identifying and providing a list of Records Management Champions for their Directorate to the Records and Information Management Officer.

4.8 Information Management Group

Oversees the development of information management and data protection measures and processes within the Council; to assure the quality of relevant processes; to consider information sharing requests and associated protocols; and to ensure learning and action is identified and progressed for all Council services and activities.

4.9 Heads of Service and Line Managers

Responsible for ensuring their staff, and where appropriate contractors and suppliers, are aware of and comply with this policy.

4.10 Third Parties

This policy and the related Records Management Document Framework must be adhered to by all third parties, contractors, volunteers and not for profit organisations performing a function on behalf of the Council.

5. Lawful Bases for Processing Personal Information

The lawful bases for processing are set out in the General Data Protection Regulation. 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.

6. Rights of Individuals

The General Data Protection Regulation 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, which is securely moving personal information from one IT place to another.
- 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.

7. The Data Protection Principles

The General Data Protection Regulation sets out six principles for the processing of personal information which are legally binding on the Council. The personal information must be:

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

The Council consistently reviews the information it holds to ensure it has a legal basis for holding the personal data we hold, and that we will also have a valid legal basis for disclosing this personal data to third parties where this happens. Privacy notices have been introduced to comply with GDPR requirements (and to reflect the legal basis of processing). Data processor agreements and data sharing agreements are being updated to reflect the new legal requirements.

7.2 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.

The purposes for which data are collected are clearly set out 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.

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

In assessing the data flows, the Council has also taken the opportunity to critically assess the need for each of the data fields in question and where superfluous data was being captured, the Council is now in the process of ceasing to capture this.

7.4 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.

The Council is continually checking data for accuracy through the Information Asset Register and, where any inaccuracies are discovered, these are promptly corrected and any third party recipients of the inaccurate data notified of the correction.

7.5 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 General Data Protection Regulation in order to safeguard the rights and freedoms of the data subject.

The Council only keeps personal information for the minimum period amount of time necessary. Sometimes this period is set out in the 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 for.

The Council follows the Scottish Council on Archives Records Retention Schedules (SCARRS) national Scottish Retention scheme for local authorities. This offers up to date legislative retention and informed business best practice retention. Legislative retention is fixed while business best practice in SCARRS is offered as a guideline to Councils.

The Council is currently developing its SCARRS-based retention Schedule as part of its MS SharePoint roll-out project. Over the coming months, the customised schedule will be posted on our website.

The Council's Archives are held subject to appropriate safeguards in terms of Article 89.

Ongoing management of the Council's records and information is subject to the provision 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. You can view this on our website at - https://www.dumgal.gov.uk/media/20972/Records-ManagementPlan/pdf/DGC_Records_Management_Plan.pdf?m=636857443390500000
The Council's Records Management Document Framework is a suite of documents that 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.

7.6 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.

The Council has an approved Information Management Strategy and an Acceptable Use of IT Policy, which sets out roles and responsibilities within the organisation in relation to information security. All staff are required to sign the Data Protection and Confidentiality Agreement for personal data and business information. This will be refreshed following approval of this Policy. Our ICT systems have appropriate protective measures in place incorporating defence in depth 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.

8. Notifying the Information Commissioner

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

9. Processing Personal Information

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.

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.

10. 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. All staff

(including supply/relief) have a confidentiality clause in their contracts of service. They also sign a Data Protection and Confidentiality Agreement on an annual basis.

Staff who work on computer systems that hold or process personal information, or who use the information associated with those systems, will receive relevant training. If written procedures for using such systems are not yet in place, staff will be trained in legitimate ways of finding and providing information and told which information must not be recorded.
Any new staff 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 member of staff in the first instance to enable appropriate arrangements to be made.

Local training modules can be put in place for service areas who routinely deal with more sensitive personal and/or confidential information.

Elected Members will be provided with training in basic data protection law and practice.

11. Information Security

The Council's approach to Information Security is set out in its Acceptable Use of IT Policy and Security Classification Scheme.

12. 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. 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's Office.

13. 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 the Data Protection Officer must immediately be informed who will put into place a Breach Management Plan. Where an IT security breach occurs, this will be reported to the Information Security Officer who will respond to it in accordance with the provisions of the ICT Policy and Procedures.

More information on breach management can be found on Dumfries and Galloway

Council's Data Protection SharePoint Site and Information Commissioner's Office Guidance on Data Security Breach Management.

14. Monitoring and Reporting

This policy will be reviewed every three years by the Data Protection Officer. Proposed changes to information governance policies or procedures will be considered by the Information Management Group in the first instance. A review of the Council's compliance with relevant legislation and best practice will be reported to Elected Members on an annual basis.

15. Related Policies and Procedures

- Dumfries and Galloway Council Records Management Plan
- Dumfries and Galloway Council Records Management Policy
- Dumfries and Galloway Council Complaints Handling Procedure

16. Further Information

Questions relating to this policy and the Council's compliance with both the legislation should be directed to the Information Governance Team:

Email: dataprotection@dumgal.gov.uk
Telephone: 030 33 33 3000

Information Governance Team
Democratic Services
Dumfries and Galloway Council
Council Offices
English Street
Dumfries
DG1 2DD

Document Control Committee Approval

Version	Committee	Committee Date
V1.0	Agreed at Policy and Resources Committee	24 January 2019

Version control

Version	Date	Summary of changes	Job Title
V1.0	24 January 2019	Published following approval	Head of Legal and Democratic Services
V2.0	21 February 2020	Section 16 Further Information updated	Information Governance Officer