Data Protection Policy

Approved Date	September 2023
Review Date	September 2025
Related Legislation/Applicable Section of Legislation	• Data Protection Act 2018 • UK General Data Protection Regulation 2018 • Freedom of Information Act 2000 • Environmental Information Regulations 2004 • The Freedom of Information and Data protection (Appropriate Limit and Fees) Regulations 2004 • Lord Chancellor's Code of Practice • The Re-use of Public Sector Information Regulations 2005
Related Policies, Procedures, Guidelines, Standards, Frameworks	• Complaints Policy • Access to Information Policy • IT Policies • Retention and Disposal Schedule
Replaces	Data Protection Policy v2.0 (2019)
Policy Lead (Name/Position/Contact details)	Policy Manager policy@midandeastantrim.gov.uk
Sponsor Directorate	Corporate Services
Version	3.0

Revision record

Date	Version	Revision Description
June 2015	1.0	Initial issue
April 2018	2.0	Policy reviewed and updated
September 2023	3.0	Policy reviewed and updated. Minor amendments to content as outlined in the schedule of amendments.

Contents Page

1 Introduction

1.1 The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 controls how the Council processes an individual's personal information or data, by requiring compliance with the Data Protection Principles; that is to ensure that personal information is:

a. Processed lawfully, fairly and in a transparent manner,
b. Collected for specified, explicit and legitimate purposes,
c. Adequate, relevant, and limited to what is necessary,
d. Accurate and where necessary kept up to date,
e. Kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which those whose data are processed, and
f. Processed in a manner that ensures appropriate security of the personal data.

1.2 Accountability is central to the UK GDPR. As a Data Controller, Council is responsible for compliance with the data protection principles and must be able to demonstrate this to data subjects and the Regulator (the Information Commissioners Office).

2 Purpose

2.1 The purpose of this policy is to ensure Mid and East Antrim Borough Council's compliance with the UK GDPR, the Data Protection Act 2018, associated legislation, and best practice in order to protect individuals regarding the processing of their personal data by Council.

3 Scope

3.1 This Policy applies to employees, elected members, agency workers, third party organisations and other authorised individuals – referred to as 'users' within this policy.

3.2 Failure to observe the standards as set out in this Policy may be regarded as misconduct and may render an employee liable to action under the MEABC disciplinary procedures.

3.3 Individuals who consider that their personal data has been processed incorrectly by Council or in any way breaches the Data Protection Principles, may complain to Council or directly to the Information commissioner's Office. Where possible, Council will manage complaints regarding data protection in line with the Complaints, Compliments and Comments Policy. The UK GDPR includes a range of sanctions which may be imposed, including financial penalties.

4 Responsibility

4.1 The Director of Corporate Services will have overall responsibility for the implementation of the Data Protection Policy. Each Director will assume responsibility for the compliance of staff within their departments. Under the Council's Information Governance Policy, all 'Information Asset Owners' have responsibility for compliance in respect of the information they process.

4.2 In compliance with Article 37 of the UK GDPR, Council has appointed a Data Protection Officer (DPO).

4.3 The Data Protection Officer (DPO) will provide fulfill the duties as outlined in Article 39 of the UK GDPR, providing advice and guidance and monitoring Council's compliance with the Regulation.

5 Lawful basis for processing

5.1 Council will identify the appropriate lawful basis for the processing for each occasion when it processes personal data.

5.2 The lawful bases for processing are set out in Article 6 of the UK GDPR and at least one of these must apply whenever we process personal data. These are:

- ***Consent***: the individual has given clear consent for you to process their personal data for a specific purpose.
- ***Contract***: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a legal contract.
- ***Legal obligation***: the processing is necessary for you to comply with the law (not including contractual obligations).
- ***Vital interests***: the processing is necessary to protect someone's life.
- ***Public task***: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- ***Legitimate interests***: the processing is necessary for your legitimate interests of the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests (this does not apply if you are public authority processing data to perform your official tasks).

5.3 Council will provide information about our lawful basis (or bases) within the applicable Privacy Notice.

5.4 Any Council Privacy Notice(s) will provide information about the intended purposes for processing the personal data.

5.5 This will apply whether we have collected the personal data directly from the individual or we have collected the data from another source.

6 Rights of data subjects

6.1 Council will ensure compliance with the rights of data subjects. Those rights are:

- The right to be informed,
- The right of access,
- The right to rectification,
- The right to erasure,
- The right to restrict processing,
- The right to data portability,
- The right to object, and
- Rights in relation to automated decision making and profiling.

7 Right to be informed

7.1 Council will inform data subjects, typically through a Privacy Notice, how information supplied to Council, whether obtained directly from the individual or not, is processed.

7.2 The information that Council will supply about the processing of personal data must be:

- Concise, transparent, intelligible and easily accessible;
- Written in clear and plain language, particularly if addressed to a child:and
  Free of charge.

8 Right to access

8.1 Under the GDPR, individuals will have the right to request:

- Confirmation that their data is being processed,
- Access to their personal data, and
- Other supplementary information – this largely corresponds to the information that should be provided in a privacy notice.

8.2 Council is required to provide a copy of the information 'free of charge'. A 'reasonable fee' may be required, or a request may be refused when it is manifestly unfounded or excessive, particularly if it is repetitive.

8.3 If a request is refused an explanation as to why will be provided and the individual will be informed of their right to complain to the Information Commissioner.

8.4 The complaint must be made to the Information Commissioner without undue delay and within one month of the refusal.

8.5 The identity of an individual must be verified to the satisfaction of Council before release of any information, most often through the provision of photographic identification.

8.6 The Council will, where possible and proportionate, provide the information requested in the preferred format of the applicant (electronic, hard copy, etc.).

8.7 Whilst individuals have the general right of access to any of their own personal information, which is held, the Council will be mindful of those circumstances where an exemption may apply and, in particular, the data protection rights of third parties who may also be identifiable from the data being requested.

8.8 Council will only disclose the data to those recipients listed in the Notification Register or where it is otherwise permitted to do so by law.

8.9 Council will seek the permission of the data subject prior to disclosure, where it is reasonable or required to do so by law.

9 Right to rectification

9.1 Council will rectify personal data where it is inaccurate or incomplete.

9.2 Where Council has disclosed the personal data concerned to others, they will contact each recipient and inform them of the rectification, unless this proves impossible or involves disproportionate effort.

9.3 A request for rectification must be made in writing and sent by post to:

Data Protection Officer
The Braid
1-29 Bridge Street,
Ballymena,
County Antrim
BT43 5EJ

A request may also be sent by email to DPO@midandeastantrim.gov.uk and will be responded to within one month from the date of receipt.

9.4 Where a request is particularly complex Council may request and extension up to an additional two months.

9.5 Where Council cannot take action for the reasons above, an explanation will be provided to the individual and they will be informed of their right to complain to the Information Commissioner and to a judicial remedy.

10 The right to erasure – also known as 'the right to be forgotten'

10.1 Where there are no compelling reasons for the continued processing of an individual's personal data, Council will delete or remove the personal data at the request of the individual.

10.2 Data may be erased to prevent processing in the following circumstance:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed,
- When the individual withdraws their consent,
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing,
- The personal data was unlawfully processed i.e., otherwise a breach of the GDPR,
- The personal data has to be erased in order to comply with a legal obligation, or
- The personal data is processed in relation to the offer of information society services to a child.

(*Under the GDPR, this right is not limited to processing that causes unwarranted and substantial damage or distress. However, if the processing does cause damage or distress, this is likely to make the case for erasure stronger*).

10.3 There are some specific circumstances where the right to erasure does not apply, and you can refuse to deal with a request.

10.4 A request for erasure may be refused where the personal data is processed for the following reasons:

- To exercise the right of freedom of expression and information,
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority,
- For public health purposes in the public interest,
- Archiving purposes in the public interest, scientific research, historical research, or statistical purposes, or
- The exercise of defence of legal claims.

10.5 Where Council has disclosed the personal data concerned to others, they will contact each recipient and inform them of the erasure of the personal data, unless this proves impossible or involves disproportionate effort.

10.6 Council will inform the individual about these recipients upon request.

11 Right to restrict processing

11.1 Council will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, we will restrict the processing until the accuracy of the personal data has been verified,
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and you are considering whether your organisation's legitimate grounds override those of the individual,
- When processing is unlawful and the individual opposes erasure and requests restriction instead, or
- If we no longer need the personal; data but the individual requires the data to establish, exercise or defend a legal claim.

11.2 Where Council has disclosed the personal data concerned to others, they will contact each recipient and inform them of the restriction on the processing of the personal data, unless this proves impossible or involves disproportionate effort.

11.3 Council will inform the individual about these recipients upon request.

11.4 Council will inform individuals if it is decided to lift a restriction on processing.

12 Right to data portability

12.1 The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services and allows them to move, copy or transfer personal data easily from one IT environment in a safe and secure was, without hindrance to usability.

12.2 The right to data portability only applies:

- To personal data an individual has provided to a Controller,
- Where the processing is based on the individual's consent or for the performance of a contract, and
- When processing is carried out by automated means.

12.3 Where the data requested meets these requirements Council will provide the personal data in a structure, commonly used and machine-readable form and free of charge.

12.4 If requested by an individual, Council will transmit the data directly to another organisation if it is technically feasible.

12.5 Council will respond without delay, and within one month from the date of the request.

12.6 This can be extended by up to two months where the request is complex, or Council has received a number of requests.

12.7 Council will inform the individual within one month of the date of receipt of the request and explain why the extension is necessary.

12.8 Where Council is not taking action in response to a request, we will explain why to the individual, informing them of their right to complain to the Information Commissioner and to a judicial remedy without due delay and at the latest within one month from the date of receipt of the request.

13 Right to object

13.1 Individuals have the right to object to:

- Processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling),
- Direct marketing (including profiling), and
- Processing for purposes of scientific/historical research.

13.2 Council will stop processing the personal data unless:

- There are compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual, or
- The processing is for the establishment, exercise or defence of legal claims.

13.3 Council will inform individuals of their right to object 'at the point of first communication' and on our privacy notice. This will be 'explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information'.

13.4 Council will stop processing personal; data for direct marketing purposes as soon as we receive an objection.

13.5 If Council is conducting research where the processing of personal data is necessary for the performance of a public interest task, we are not required to comply with an objection to the processing.

14 Rights related to automated decision-making including profiling

14.1 Council does not currently utilise automated decision-making, including profiling.

15 Elected Members and Council Officers

15.1 Elected Members and Council Officers as data subjects.

a. Council will ensure that all Elected Members and Officers are advised of their rights as data subjects under the UK GDPR; and

b. Officers are not required to submit a subject access request to view their personnel file or to receive a copy of their job description.

15.2 Information held on Council owned equipment.

a. All information held on Council equipment (including PCs, Laptops, Mobile telephones, electronic organisers, recording pen or other recording device etc.) may be subject to an information search in the course of processing a subject access request or information request made under the Freedom of Information Act 2000 or Environmental Information Regulations 2004;

b. Elected Members and Officers are therefore advised not to hold sensitive personal information on any Council equipment without ensuring the need to hold the information and ensuring appropriate security measures are in place.

15.3 Information held on personal equipment.

a. Council data must not be held on personal equipment (including PCs, Laptops, Mobile telephones, electronic organisers, recording pen or other recording device etc.) belonging to Elected Members or Council Officers;

b. Where Council data is being held on personal equipment (including PCs, Laptops, Mobile telephones, electronic organisers, recording pen or other recording device etc.) these may also be subject to an information search in the course of processing a subject access request or information request made under the Freedom of Information Act 2000 or Environmental Information Regulations 2004.

16 Security

16.1 Council will ensure that:

- Appropriate security measures are in place to protect personal data, both automated and manual systems,
- Personal data systems are accessible to authorised staff only, and
- Authorised staff using these systems will be advised of appropriate security procedures and the importance of their role within these procedures.

16.2 Care should be taken in the use of email for the transmission of sensitive personal information. Where necessary, emails containing sensitive personal information must be transmitted using appropriate security measures.

16.3 Hard copy files that contain personal information will be stored in a secure location with controlled access. When a file is moved from storage the Officer doing so will be responsible for its safe keeping at all times, particularly when taken into a public location.

16.4 Use or removable electronic media (e.g., USB sticks, portable hard drives etc.) will be in accordance with the relevant Council ICT Policy.

17 Incident reporting

17.1 Council has the responsibility to monitor all incidents that may breach the security/confidentiality of information. Any such incidents must be reported to the Data Protection Officer immediately upon the discovery of the breach.

17.2 The Data Protection Officer will be responsible for the recording, investigation and risk assessment of all data protection related incidents and for any communication with the Information Commissioners Office.

17.3 The Data Protection Officer will report to the Senior Management Team annually on all breaches, and will inform SMT in real time in each instance that there is a breachwhich is required to be reported to the Information Commissioners Office and/or the affected data subjects.

17.4 In all incidents of breach or potential breach, the ICO Guidelines on Information Security Incident Reporting must be followed.

18 Risk Management

18.1 The accidental or deliberate disclosure of 'sensitive' personal information or the retention of personal information for longer than required poses a potential risk to the Council.

18.2 Actions to manage any risk will be identified, implemented and reviewed regularly as part of the overall Risk Management process.

19 Training

19.1 Council will ensure that all Council Officers with responsibility for processing personal data are appropriately trained and aware of their data protection obligations and liabilities under the UK GDPR and the Data Protection Act 2018.

20 Communicating the policy

20.1 The Data Protection Policy will be clearly communicated and accessible to all of the Council's customers and stakeholders.

20.2 The team responsible for Information Governance deliver a programme of training on Data Protection and are available to provide tailored sessions to address specific departmental needs.

20.3 All Elected Members and staff will have access to this policy and supporting material on the shared drive or MinutePad.

21 Monitoring and Review

21.1 The Data Protection Officer will monitor this policy on an ongoing basis and review the policy document bi-annually to ensure that it reflects any:

- Changes in legislation, Codes of Practice,
- Changes to Council Policies,
- Introduction of new technology,
- Identification of increased risks,
- Identification of system vulnerabilities,
- Data breach, or
- Weakness in the Policy being identified.