Data Protection Policy

Approved Date	8 May 2018
Review Date	May 2020
Related Legislation/Applicable Section of Legislation	General Data Protection Regulation Data Protection Act 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	
Policy Lead (Name/Position/Contact details)	Head of Corporate Services
Sponsor Directorate	Chief Executive's Office
Version	2.0

Contents

1. Introduction

1.1 The General Data Protection Regulation (GDPR) controls how the Council processes an individual's personal information or data by requiring compliance with the Data Protection Principles; that is to ensure 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 is necessary for the purposes for which those data are processed; and
f. Processed in manner that ensure appropriate security of the personal data.

1.2 Accountability is central to GDPR. As a data controller Council is responsible for compliance with the principles and must be able to demonstrate this to data subjects and the regulator (the Information Commissioner).

2. Purpose

2.1 The purpose of the Data Protection Policy is to ensure Mid and East Antrim Borough Council's compliance with the GDPR, the Data Protection Act 2018 and associated legislation/good practice to protect individuals with regard to 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 comply with this policy may result in disciplinary action.

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 the Information Commissioner's Office after exhausting the internal Council complaints process (line manager, Director, Chief Executive). GDPR includes a range of sanctions which may be imposed, including financial penalties.

4. Responsibility

4.1 The Chief Executive will have overall responsibility for the implementation of the Data Protection Policy. Each Director will assume responsibility for the compliance of staff within their department.

4.2 The Data Protection Officer will provide advice and guidance on implementation of GDPR and the Data Protection Policy.

5. Lawful basis for processing

5.1 Mid and East Antrim Borough Council will identify the lawful basis for processing personal data.

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

- ***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 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 or 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 a public authority processing data to perform your official tasks.)

5.3 Council will provide information about our lawful basis (or bases) within a privacy notice.

5.4 Council privacy notice(s) will provide information about the intended purposes of processing the personal data and the lawful basis for processing.

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 The 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
- Rights in relation to automated decision making and profiling.

7. Right to be informed

7.1 Mid and East Antrim Borough 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 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 obtain:

- 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 will 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 the Information Commissioner.

8.4 The Information Commissioner should be informed without undue delay and within one month from the date of refusal.

8.5 The identity of an individual will be verified before release through the provision of photographic identification.

8.6 Mid and East Antrim Borough Council will where possible and proportionate provide the data requested in the preferred format of the applicant.

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

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

9. Right to rectification

9.1 Mid and East Antrim Borough Council will rectify personal data where it is inaccurate or incomplete.

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

9.3 A request for rectification can be made via email at policy@midandeastantrim.gov.uk and will be responded to within one month.

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

9.5 Where Council cannot take action to rectify 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 is no compelling reasons for the continued processing of an individual's personal data, Mid and East Antrim Borough Council will delete or remove the personal data at the request of the individual.

10.2 Data may be erased to prevent processing in following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws 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 (ie otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- 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 or defence of legal claims.

10.5 If the personal data in question has been disclosed to others, we will contact each recipient and inform them of the erasure of the personal data - unless this proves impossible or involves disproportionate effort.

10.6 Upon request Mid and East Antrim Borough Council will inform the individual about these recipients.

11. Right to restrict processing

11.1 Mid and East Antrim Borough 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.
- 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 the personal data in question has been disclosed to others, we 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 If asked to, we will also inform the individuals about these recipients.

11.4 Council will inform and 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 to another in a safe and secure way, 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 There the data requested meets these requirements Mid and East Antrim Borough Council will provide the personal data in a structured, commonly used and machine readable form and free of charge

12.4 If the individual requests it, Council will transmit the data directly to another organisation, if this is technically feasible.

12.5 Council will respond without undue delay, and within one month.

12.6 This can be extended by two months where the request is complex or we have received a number of requests.

12.7 Council will inform the individual within one month of the 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 undue delay and at the latest within one month.

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 and statistics.

13.2 Mid and East Antrim Borough Council will stop processing the personal data unless:

- There is 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 in 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 Council will inform individuals of their right to object "at the point of first communication" and in 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".

13.6 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 Mid and East Antrim Borough 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

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

ii. Officers are not required to submit a subject access request to view their personnel file or to receive a copy of standard documentation such as their job description.

15.2 Information held on Council owned equipment

i. All information held on Council equipment (including PCs, laptops, mobile phones, electronic organisers) may be subject to an information search in the course of processing a subject access request or information request made under Freedom of Information Act 2000 or Environmental Information Regulations 2004.

ii. Elected Members and Officers are therefore advised not to hold sensitive personal information on 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

i. Council data held on an Elected Members or Council Officers personal equipment (including home PCs, laptops, mobile phones etc) may also be subject to search.

16. Training

16.1 Council will ensure that all Council Officers with responsibility for the processing of personal data are appropriately trained and aware of their data protection obligations and liabilities under the Act.

17. Security

17.1 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;
- Authorised staff using these systems will be advised of appropriate security procedures and the importance of their role within these procedures.

17.2 Care should be taken in the use of email for the transmission of sensitive personal information. Where necessary, emails containing sensitive personal information should be encrypted or information sent in hard copy in sealed envelope via internal mail.

17.3 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.

17.4 Use of removable electronic media (USB sticks, portable hard drives etc) will be in accordance with the Council's ICT policies.

18. Incident reporting

18.1 Council has responsibility to monitor all incidents that may breach security/confidentiality of information. Any such incidents will be reported to the relevant Director for investigation and Head of Policy, Research and External Affairs for monitoring purposes.

18.2 In incidents of breach or potential breach the Guidelines on Information Security Incident Reporting (Appendix C) should be followed.

19. Risk Management

19.1 The accidental or deliberate disclosure of "sensitive" personal information or the retention of personal information for longer than required pose a potential risk to the Council.

19.2 Actions to manage this risk will be identified, implemented and reviewed regularly as part of the risk management process.

20. Review

20.1 This Policy will be reviewed regularly, and at least annually, to ensure that it reflects any:

- Changes in legislative requirements;
- Changes in Government directives or Codes of Practice;
- Changes in Council Policy; and/or
- Weaknesses in the Policy being highlighted.

Appendix A

Glossary of Terms

Data	Information which: • Is processed by means of equipment operated automatically in response to instructions given for that purpose; or • Is recorded with the intention that it should be so processed; or • Is recorded as part of a relevant structures filing systems or with the intention that it will form part of a system; or • Is recorded information held by the Council which does not fall within the three points above. Automated data: • Computer records; • Audio/video; • CCTV and digitised images; • Document image processing Manual data: • Paper files; • Card index systems; • Microfiche records.
Data Controller	The person in the Council who determines the purposes for which personal data is to be processed and the manner in which this is to be processed
Data Processor	Any other person who processes the data on behalf of the Data Controller.
Data Subject	An individual who is the subject of the data held
Personal data	Information which relates to an individual who is: • Living; • Identifiable (from that data of from other data held by the Data Controller).
Processing	Obtaining, recording or holding data or carrying out any operation or set of operations on the data including: • Organisation, adaptation or alteration; • Retrieval, consultation or use; • Disclosure by transmission, dissemination or otherwise making available; • Alignment, combination; • Blocking, erasure or destruction.

Recipient	Any person to whom data is disclosed including any person to whom it is disclosed in the course of processing (e.g. an employee or agent of the data controller)
Structured filing systems	Any set of information relating to individuals where – although the information is not automatically processed – the set is structured either by reference to individuals or by reference to criteria relating to a particular individual is readily accessible.
Sensitive Personal Information	Personal data relating to: • Racial or ethnic origin; • Political opinions; • Religious beliefs or beliefs of a similar nature; • Membership of a Trade Union; • Physical or mental health; • Sexual life; • Criminal offences; • Criminal proceedings and convictions; • Financial information; • Genetic; and • Biometric.
Third Party	Any person other than: • The data subject; • The data controller; • The data processor or other persons authorised to process data for the data controller or processor

Appendix B

Personal information held on Council owned equipment

All information held on Council equipment (including, PCs, smartphones, mobile phones and electronic organisers) may be subject to search, for example, in the course of processing Data Protection subject access requests and/or Freedom of Information requests.

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

Elected Members and Council Officers are reminded that:
The content of an email is subject to all applicable UK laws such as those relating to copyright, defamation, data protection and public records; and

If you keep copies of email or other communications for any length of time, you should be aware that they are almost certain to be “personal data” within the terms of GDPR, i.e. email address.

Appendix C

Data Breach Incident Handling – Guidelines

1. Introduction

1.1 The Council has responsibility to monitor all incidents that occur within the organisation that may breach security/confidentiality of information.

1.2 All incidents need to be identified, reported, investigated and monitored. It is only by adopting this approach that the Council can prevent reoccurrence of such incidents.

NOTE:
These guidelines do not apply to serious incidents where the principles of computer forensics should be applied to ensure that evidence is gathered is admissible in court. In such cases the appropriate Data Protection Officer will seek professional advice/assistance, including from the Police Service of Northern Ireland (PSNI) where necessary.

2. Types of information security incidents

2.1 Breaches of information security/confidentiality could potentially compromise business operations and be damaging to the Council as a whole. Such breaches could also pose a threat to the personal safety or privacy of an individual(s) and lead to disciplinary action and possibly legal sanctions.

2.2 Examples of these types of incidents include:

- Damage to or theft/loss of information (either manual or electronic);
- Leaving confidential information/records in a public area;
- Incorrect disposal of confidential waste;
- Unauthorised access to information;
- Unauthorised disclosure of confidential information in any format including verbally;
- Transfer of information to the wrong person (by email, fax, post or phone);
- Sharing of computer IDs and passwords.

2.3 Every breach must be taken seriously and reported according to the process as follows. If there is any doubt about what constitutes a security incident, staff should contact the Data Protection Officer.

3. Reporting of incidents

3.1 Any incident or suspected incident must be reported immediately to a line manager as an information loss/breach. If the member of staff prefers to remain anonymous, a name need not be supplied.

3.2 This may involve staff reporting observed or suspected incidents or actions of others where security is threatened (see the Whistleblowing Policy).

4. Incident investigation, recording and outcomes

4.1 The Data Protection Officer will make an initial assessment of the significance of the loss and whether further action and/or investigation is warranted – to include an assessment of potential adverse consequences for individuals and how likely these are to happen.

4.2 The Data Protection Officer will establish who needs to be made aware of the breach and action for containment, including notification of affected individuals and relevant organisations.

4.3 If a large number of people are affected or there are potentially very serious consequences arising for the breach, the Information Commissioner's Office (ICO) will be informed and if appropriate the PSNI.

4.4 Notification of individuals, organisations and the ICO will be carried out in accordance with the ICO guidance on data security breach management.

4.5 Where appropriate, the Data Protection Officer or nominee will lead an investigation to establish the circumstances of the incident, the extent of any loss and the implications for Council.

4.6 Where the Data Protection Officer assesses that an independent investigation is required, for example in the event of a significant incident or where the circumstances are particularly complex, Internal Audit may be asked to lead a more thorough investigation, which may involve interviewing staff or third parties involved.

4.7 Where an incident has occurred through a staff member's failure to apply Council policy with respect to information management the Head of Human Resources and Organisation Development may be consulted. Negligent or malicious action by an employee resulting in a data breach may lead to disciplinary action.

4.8 Where an incident has occurred in respect of an Elected Member concerning information management this may constitute a breach of the Code of Conduct for Councillors and the Commissioner for Complaints may be contacted.

4.9 A report will be produced by the Data Protection Officer or Internal Audit, setting out the circumstances, extent and implications of the incident together with recommendations for preventing any subsequent similar incident, where relevant.

4.10 Significant incidents will be reported to the Information Commissioner and the Audit and Scrutiny Committee.

4.11 The Data Protection Officer will take action to ensure that lessons learned from the incident are applied to existing policies and practices. This may include implementing changes to or introducing additional systems of control, increasing awareness of information risk, or disseminating lessons learnt.

4.12 The Data Protection Officer will ensure incidents are logged to enable a central register to be maintained of all incidents occurring within the organisation.

5. Theft/loss of IT Equipment

5.1 All incidents relating to breaches of security and confidentiality where there has been a theft/loss of IT equipment must be reported immediately.