Data Protection Policy

Approved Date	June 2015
Review Date	June 2017
Related Legislation/Applicable Section of Legislation	Data Protection Act 1998 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)	Chief Executive
Sponsor Directorate	Chief Executive's Office
Version	1.0

Contents

1. Introduction

1.1 The Data Protection Act 1998 (DPA) 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:

i. Fairly and lawfully processed;
ii. Processed for the limited purposes and not processed in any manner incompatible with those purposes;
iii. Adequate, relevant and not excessive to the required purpose;
iv. Accurate and up-to-date;
v. Not kept for longer than necessary;
vi. Processed in accordance with the data subject's rights;
vii. Kept secure; and
viii. Not transferred to another country(ies) without adequate protection for the information.

1.2 The DPA is designed to protect individuals from:

- The use of incorrect information held about them;
- The improper use of correct information held about them; and
- Generally to ensure compliance with the European Directive on the protection of individuals with regard to the processing of personal data.

2. Purpose

2.1 The purpose of the Data Protection Policy is to ensure Mid and East Antrim Borough Council's compliance with the Data Protection Act 1998 (as amended) and associated legislation/good practice to protect individuals with regard to the processing of their personal data by Council.

3. Scope

3.1 The policy applies to Elected Members and Council Officers who process personal data and who themselves are the subjects of personal data processing.

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). DPA 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 Head of Policy, Research and External Affairs will provide advice and guidance on implementation of the Act.

5. Access by Data Subjects

5.1 The Council will ensure compliance with the rights of data subjects in accordance with Data Protection Principle 6, namely to:

- Have a copy of information held;
- Have it corrected if it is inaccurate, lost or disclosed in inappropriate circumstances claim compensation if they suffer damage or distress because of information being inaccurate, lost or disclosed in in appropriate circumstances;
- Prevent processing likely to cause damage or distress;
- Prevent processing for the purposes of direct marketing;
- Be informed by the Data Controller of the logic involved in any automatic decision making (i.e. the processing of personal data by automatic means for the purpose of evaluating matters relating to the individual where such processing has formed the sole basis for any decision significantly affecting that person).

5.2 A standard fixed charge of £10 will be applied to all subject access requests. This fee, together with proof of identity, will be required before work will begin on processing any request.

5.3 Council will respond positively and promptly to subject access requests, replying as quickly as possible within the 40 calendar day time limit. The timing of the processing of requests will begin from the date of receipt of the fee.

5.4 Payment of the standard fixed charge does not provide a guarantee that all information requested will be provided, nor will any refund be given if the release of information is eventually refused.

5.5 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.

5.6 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.

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

6. Elected Members and Council Officers

6.1 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 the Act.

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. Requests for other information, however, such as interview notes, salary records etc may be subject to the £10 fee.

6.2 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.

6.3 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.

7. Training

7.1 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.

8. Security

8.1 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.

8.2 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.

8.3 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.

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

9. Incident reporting

9.1 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.

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

10. Risk Management

10.1 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.

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

11. Review

11.1 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; and • Criminal proceedings and convictions • Financial information
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 date” within the terms of the Data Protection Act, 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 Director 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 Head of Policy, Research and External Affairs.

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 Director of Finance and Governance 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 Director of Finance and Governance and Head of Policy, Research and External Affairs 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 Director of Finance and Governance 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 Director of Finance and Governance judges 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 Director of Finance and Governance 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 Audit and Scrutiny Committee.

4.11 The Director of Finance and Governance 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 Head of Policy, Research and External Affairs 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.