General Data Protection Regulations Policy

DCSDC Policy	
Document Number	
Responsible Officer	Lead Democratic Services and Improvement Officer (Ext 6704)
Contact Officer	Data Protection Officer (Ext 4310)
Approval	Governance and Strategic Planning Committee – date – min ref- Council – date ratified
Effective Date	Date this approved version of the policy comes into effect.
Modifications	None
Superseded Documents	None
Review Date	To be reviewed in April 2020. However, the policy will be reviewed sooner in the event of any one or more of the following: • Failure or weakness in the policy is highlighted • Changes in legislative requirements Changes in Government/ Council or other directives and requirements.
File Number	
Associated Documents	Internet and email policy Subject Access Request Form Explanatory Notes for Subject Access Request Screening questionnaire

Contents

1. Preamble

1.1. Purpose

Derry City and Strabane District Council is obliged to comply with the General Data Protection Regulations (GDPR) 2018. GDPR is a new legal framework which replaces the existing Data Protection Act 1998. There are many similarities between the two, however GDPR is intended to bring uniformity to how data is handled across the European Union (EU).

The Information Commissioner, who oversees compliance and promotes good practice, requires all Data Controllers and Data Processors to be responsible and accountable for their processing activities. Both must comply with six data protection principles to ensure that they cover all the rights that individuals have.

The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals within the EU.

This document sets out Derry City and Strabane District Council's policy and the controls used in complying with its statutory obligations.

1.2. Background

The GDPR give individuals the right to see information about them held by companies and organisations. In certain circumstances they may have the information corrected or erased, or they may even be able to prevent the processing of their personal data.

If a Data Controller or Data Processor causes an individual damage or distress, as a result of non-compliance, they could claim compensation. The Council is classed as a Data Controller and could be prosecuted for any serious offences that may be committed. Under GDPR the potential fine could be up to €20m.

2. Scope

This policy applies to all personal data held by Derry City and Strabane District Council. It encompasses manual/paper records and personal data electronically

processed including information gathered on CCTV systems, of whatever type and at whatever location, used by or on behalf of the Council.

The obligations outlined in this policy apply to all those who have access to personal data held by Derry City and Strabane District Council, whether employees, agency staff, elected members (or other representatives).

Any individual who knowingly or recklessly processes data for purposes other than those for which it is intended or is deliberately acting outside of their recognised responsibilities may be subject to the Council's disciplinary procedures, including dismissal where appropriate, and possible legal action.

All individuals permitted to access personal data in line with their work duties must agree to comply with this policy and agree to undertake any relevant training that may be appropriate to the job/position being undertaken.

As well as the Council, individual employees / members can also be prosecuted for unlawful action under the Act. Upon summary conviction (in a Magistrate's Court), fines of up to £5000 could result if employees /members process information about other people without their consent or proper authorisation from the Council. Upon conviction or indictment (Crown Court), the fine can be unlimited.

Employees/ members could be committing an offence by sharing information with others who do not need that information in order to carry out their legitimate Council duties.

3. Definitions

Data: Any information that is:

- Being processed by means of equipment operating automatically in response to instructions given for that purpose (e.g. payroll system)
- Recorded with the intention that it should be processed by means of such equipment
- Recorded as part of a manual filing system or with the intention that it should form part of a relevant filing system
- One of a number of records to which public access is allowed.

Personal Data: Personal data is defined as, data relating to a living individual who can be identified from:

- That data;
- That data and other information which is in the possession of, or is likely to come into the possession of the data controller and includes an 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.

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This can include:

- identification number, location data or online identifier. This reflects changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Special Category Personal Data: is defined as personal data consisting of information as to racial or ethnic origin; political opinion; religious or other beliefs; trade union membership; physical or mental health or condition and sexual life.

The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

Data Subject: An individual who is the subject of the personal data.

Data Controller: means the Council - as the organisation that decides the manner in which, and purpose for which, personal data (including CCTV) are processed.

Data Processor: An individual or organisation who is responsible for processing personal data on behalf of a controller.

Processing: any activity/operation performed on personal data - whether held electronically or manually, such as obtaining, recording, holding, disseminating or making available the data, or carrying out any operation on the data. This includes, organising, adapting, amending and processing the data, retrieval, consultation, disclosure, erasure or destruction of the data.

<u>It is difficult to envisage any activity carried out by the Council which does not amount to processing.</u>

Information Commissioner: an independent Officer appointed to oversee the implementation of the GDPR legislation.

Relevant filing system: a relevant filing system exists where records relating to individuals are held in a sufficiently systematic, structured way as to allow ready access to specific information about those individuals.

4. Policy Statement

In order to operate efficiently, Derry City and Strabane District Council has to collect and use information about individuals. This 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 in order to comply with the requirements of central government and other bodies.

This personal information will be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means, and there are safeguards within the new Data Protection Bill to ensure this.

Derry City and Strabane District Council regards the lawful and correct 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 correctly.

To this end, the Council fully endorses and adheres to the Principles of Data Protection as set out in the General Data Protection Regulations. Disciplinary or other action may be taken against any employee or member who breaches any aspect of this policy or the procedures for its implementation.

4.1 Roles and Responsibilities

Overall responsibility for the efficient administration of the Data Protection legislation lies with the **Chief Executive.** Operational implementation will be coordinated by the Lead Democratic Services and Improvement Officer.

Day to day responsibility for administration and compliance with the Act/Regulations is delegated to **Directors, Heads of Service and Lead Officers**, for compliance with the Act/Regulation's provisions within their respective areas of authority.
Data Protection Officer - It is the responsibility of the Data Protection Officer to assist the Council to ensure compliance with this policy, to specify the procedures to be adopted and to co-ordinate any associated data collection required as part of a Data Protection request. The main duties of the Data Protection Officer are:-

- maintenance of the Council's external registration/notification under the Act, and as interface with the Data Protection Registrar/Commissioner
- development, update and publication of data protection procedures for the Council
- maintenance of the internal register of sources and disclosures and to audit data protection procedures and practices
- initial contact point for subject access requests
- in conjunction with the Training Officer, provision of education and training seminars regarding data protection issues

Digital Services Manager- The main duties of the Digital Services Manager are to: -

- Develop and enforce the Internet and E-mail Policy and Guidelines

- Ensure that appropriate systems are in place to protect the security and integrity of electronic data and enhance accessibility.

All employees – all employees now have personal responsibility to ensure that they adhere to Council policies around Data Protection.

4.2 General Principles

The General Data Protection Regulations stipulate that anyone processing personal data must comply with **Six Principles** of good practice. These Principles are legally enforceable.

The Principles require that personal information is:

- processed lawfully, fairly and in a transparent manner in relation to individuals;

- 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;

- adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

- 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;

- 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 individuals; and

- 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.

4.3 Confidentiality and Security

Personal data is confidential and confidentiality must be preserved in compliance with the GDPR principles outlined in 4.2 above. Confidential information can be the most valuable asset of a business and employees will automatically have duties to their employers to ensure that confidential information is not knowingly or recklessly misused. Accordingly, where personal data is stored in -

- **Manual files** (paper records) - access must be restricted solely to relevant staff and stored in secure locations (e.g. lockable cabinets), to prevent unauthorised access.

- **Electronic files** - Computer systems will be configured and computer files created with adequate security levels to preserve confidentiality. Those who use the Council's computer equipment will have access only to the data that is both necessary for the work they are doing and held for the purpose of carrying out that work.

Personal data will be disclosed only to the data subject and other organisations and persons who are pre-defined as notified recipients within the Council's Notification Register Entry held with the Information Commissioners Office.

At certain times it may be required that personal data be disclosed under one of the exemptions within the General Data Protection Regulations. If there is a requirement for this, an audit trail will need to be kept to provide accurate records of any disclosures of personal data.

The Council will process **special category personal data** (as defined in the Regulations) of employees and service users in accordance with monitoring arrangements defined under the Fair Employment and Treatment (Northern Ireland) Order 1998, in the Council's Policy and Procedures for the Protection of Children and Vulnerable Adults and in the Equality Commission's 'Section 75 Monitoring Guidance for Use by Public Authorities'.

4.4 Ownership of Data

Each Council Directorate is responsible for the personal data that it holds. This responsibility also extends to personal data that is processed by a third party on behalf of the Council. The Directorate will hold a record of all processing activities containing personal data, whether paper based or electronic. Where required, the Directorate will provide the necessary information to the Data Protection Officer in order to facilitate the notification of the data with the Information Commissioner.

4.5 Processing data

All processing of personal data will comply with the Data Protection Principles as outlined in 4.2. In the situation where a third party processes data, the third party will be required to act in a manner which ensures compliance with the General Data Protection Regulations and have adequate safeguards in place to protect the personal data.

Data will only be processed for the purpose for which it was collected and should not be used for additional purposes without the consent of the data subject.

The Council is obliged to inform all individuals of why their personal data is being collected. In line with the first data protection principle, all information will be

collected fairly and lawfully and processed in line with the purpose for which it has been given.

The Council may need to hold and process information in order to carry out any statutory obligations, where this process takes place, all personal data will be processed fairly and lawfully.

It is a requirement that any data collection forms used in order to collect personal data will contain a "lawful basis for processing" statement.

The statement will need to be clearly visible and placed appropriately so the data subject (individual to whom the information relates) is fully aware of the intended uses of their personal data.

Council forms may also need to include a section where explicit and specific consent, to use their personal data, is given by the data subject.

The information that would need to be supplied on a data collection form is as follows:

- The Council's identity
- The identity of the Data Protection Officer or appointed representative
- The purpose or purposes for which the information is intended to be processed
- The lawful basis for processing personal data
- Any foreseen disclosures of the information to be obtained; and
- Any further information in order to make the processing fair.
- A specific section that allows consent to be given (where required)

It is also very important to remember that when collecting data via the telephone or face to face the above information should also be made clear to the data subject before any processing of their personal data takes place.

Personal data must not be disclosed, except to **authorised** users, other organisations and people who are pre-defined as a **notified recipient** or if required under one of the **exemptions** within the General Data Protection Regulations.

4.6 Data Subject Rights

4.6.1 The Right to be informed

An individual has the right to be provided with "fair processing information" usually through a Privacy Notice. This emphasizes the need for transparency over how we use personal data.

4.6.2 The Right of Subject Access

A written request (letter, email etc.) received by the Council from an individual wishing to access their rights under the provisions of the General Data Protection Regulations is known as a Subject Access Request.

Individuals have the right to request access to any 'personal data' that they believe may be held about them. They also have the right to know why we hold it and who we disclose it to.

If we do hold the requested information, we will provide a written copy of the information held about them and details of any disclosures which have been made. The information requested will be provided promptly and in any event **within one calendar month of receipt** of the subject access request.

If the information cannot be disclosed within the time period specified, the data subject will be kept fully informed of the process and given access to any personal data that may already have been gathered.

The GDPR state that individuals have a right to access their personal data so a fee cannot normally be charged for a Subject Access Request. However, we can charge a ‘reasonable fee’ when a request is manifestly unfounded or excessive, particularly if it is repetitive.

If the data subject believes that Derry City and Strabane District Council has not responded correctly and are not happy with our response to their concerns they are able to complain to the Information Commissioner.

4.6.3 The Right to be forgotten/erasure

If an individual believes that we are processing personal data that is no longer required in relation to the purpose for which it was originally collected or if substantial unwarranted damage or substantial unwarranted distress is being caused, they can ask the Council to stop the processing. This is their right to erasure.

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

4.6.4 The Right to Object

An individual is entitled to ask the Council (in writing) to cease, or not to begin, processing their personal data for any purpose unless we can demonstrate 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.

When we receive a written notice we must comply as soon as practically possible.

An individual may apply to a Court for an order if the data controller fails to comply with a written notice.

If we do not have a “legitimate interest” or “valid lawful” grounds for processing data we will seek the explicit affirmative consent of the data subject to do so. Where consent has been given, it can be withdrawn at any time by the data subject without bias. We must clearly show the data subject how to do this.

4.6.5 The Rights in relation to automated decision taking

An individual is entitled, by written notice, to require a data controller to ensure that no decision, which significantly affects that individual, is based solely on the processing, by automatic means, of personal data of which that individual is the data subject.

We will carry out a Data Protection Impact Assessment (DPIA) to consider and address the risks before we start any new automated decision-making or profiling.

4.6.6 The Right to compensation

An individual who suffers damage, or damage and distress, as the result of any contravention of the requirements of the Act by a data controller, is entitled to compensation where the data controller is unable to prove that they had taken such care as was reasonable in all the circumstances to comply with the relevant requirement.

4.6.7 The Right to rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. A data subject can ask for the data controller to rectify, block, erase or destroy such data relating to that data subject as are inaccurate together with any other personal data relating to the data subject which contain an expression of opinion based on the inaccurate data.

4.6.8 The Right to Data Portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

It 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.

We must provide this information free of charge and within one month of receiving a request.

4.6.9 Re-use of Public Sector Information

The Re-use of Public Sector Information Regulations 2005 established a framework for making the re-use of public sector information easier and more transparent. The main aims of the Regulations are:

- Fairness
- Transparency
- Timing
- Openness
- Consistency

Re-use means the use by a person (or company) of a document held by the Council for a purpose other than the initial purpose for which the document was produced.

To be valid, a request for re-use of Public Sector Information must:

- Be in writing
- State your name and address
- Specify the document which you want to re-use
- State the purpose for which the document is to be re-used

We will respond to a request within 20 days of receipt. If we need more time we will inform the requester.

5. Legal & Policy Framework

5.1 Linkage to Corporate Plan

The Corporate Plan 2017-18 highlights the strategic objective of “an effective, efficient, accountable and transparent organisation”. Systems that ensure the security and proper use of personal information are key to achieving this objective.

5.2 Legal Context

This policy directly relates to compliance with the General Data Protection Regulations 2018. There are also a number of other pieces of relevant legislation, including:

- The European Union Data Protection Directive (95/46/EC)
- Northern Ireland Act 1998
- Fair Employment and Treatment (Amendment) Regulations (Northern Ireland) 2003
- The Freedom of Information Act 2000

6. Impact Assessment

6.1 Screening and Equality Impact Assessment

This draft policy has been screened out for equality impact assessment.

6.2 Impact on staff and financial resources

A formal policy on data protection has been in place for a number of years and consequently it is not envisaged that there will be any significant ongoing implementation issues in regard to staff and financial resources.

In the short term, however, resources will be required to make staff aware of the new GDPR and in reviewing existing data protection processes. It is considered that these requirements can be met within existing resources.

6.3 Sustainable Development

In so far as this policy promotes engagement of citizens through the safeguarding of personal data and the building of service users' trust in the organisation, there is a positive contribution towards the Sustainable Development Duty.

6.4 Other impacts

The adoption of a formal policy will facilitate a more robust and standardized approach to dealing with personal data across the organization. It will also help ensure that control measures are in place to facilitate online transactions via the Council's web-site.

7. Implementation

Overall responsibility for the implementation of this policy lies with the Chief Executive. Operational implementation will be coordinated by the Lead Democratic Services and Improvement Officer.

The Data Protection Officer to assist the Council to ensure compliance with this policy, to specify the procedures to be adopted and to co-ordinate any associated data collection required as part of a Data Protection request.

7.1 Support and Advice

7.1.1 Training

It is the Council's policy that all employees who hold or process personal data receive the appropriate training in order to comply with the GDPR.

Data Protection training is a crucial element of staff awareness. Staff need to be aware of their obligations relating to any personal data they process as part of their

Council duties. Failure to adhere to the six data protection principles can lead to serious problems and prosecution.

7.1.2 Advice

Further information on this policy and advice in relation to data protection issues can be obtained from the Data Protection Officer. Specialist legal advice can be obtained from the Lead Legal Services Officer.

7.2 Communication Strategy

Responsibility for the communication of this policy lies with the Data Protection Officer. Copies of the policy, once approved will be made available on the Council's intranet site. Training will be arranged in conjunction with the HR Section.

7.3 Risk Management

Failure to comply effectively with this policy may lead to the loss or inappropriate use of personal data. Whilst experience indicates that the likelihood of such an occurrence is low, each Council department will review its current arrangements in relation to the processing of personal data within 6 months of the approval of this policy.

8. Monitoring, review and evaluation

This policy will subject to review no later than 3 years after approval.

9. Acknowledgements