



Fermanagh & Omagh
District Council

Comhairle Ceantair
Fhear Manach agus na hÓmaí

Data Protection Policy

Introduction

Fermanagh and Omagh District Council needs to collect and use information about people with whom it works in order to operate and carry out its functions. These may include members of the public, current, past and prospective employees, clients and customers and suppliers. In addition, the Council may be required to collect and use information in order to comply with legislative requirements. This personal information must be handled and dealt with properly however it is collected, recorded and used and whether it is on paper, in computer records or recorded by other means.

Aim

The aim of the policy is to set out the Council's commitment to protecting personal data and how we will ensure that staff understand how to handle data they have access to a part of their work.

3 Objectives

By working in accordance with this Policy and the supporting Framework, Fermanagh and Omagh District Council will:

3.1 comply with the Data Protection Act 2018 and General Data Protection (GDPR) principles and ensure that personal data is:

- Processed fairly and lawfully and in a transparent manner
- Obtained for one or more specified, explicit and lawful purposes
- Adequate, relevant and only limited to what is required
- Accurate and where necessary kept up to date
- Not kept in a form which permits identification of data subjects for longer than is necessary
- Processed in accordance with the rights of data subjects
- Processed in a manner that ensures appropriate security of the personal data, and

3.2 ensure that the rights of people about whom information is held can be fully exercised in accordance with legislative requirements. These rights are:

- The right to be informed
- The right of access to personal information
- The right to request rectification
- The right to request erasure
- The right to restrict processing in certain circumstances
- The right to data portability
- The right to object to processing, and
- Rights related to automated decision making and profiling.

4 Scope

To ensure the successful implementation of the Data Protection Policy and Framework, clear roles and responsibilities have been identified.

Group or Individual	Role and Responsibilities
Councillors	<ul style="list-style-type: none"> ➤ Approve the Data Protection Policy and subsequent amendments. ➤ Attend any relevant training or awareness raising sessions. ➤ Act in accordance with the Policy and Framework at all times.
Chief Executive	<ul style="list-style-type: none"> ➤ The Chief Executive has ultimate officer responsibility for embedding Data Protection principles throughout the Council.
Senior Management Team	<ul style="list-style-type: none"> ➤ Allocate resources to enable the Council to meet its responsibilities. ➤ Promote the integration of Data Protection principles into the culture of the Council. ➤ Consider related issues at SMT meetings.
Heads of Service	<ul style="list-style-type: none"> ➤ Ensure employees are aware of this policy. ➤ Notify the Data Protection Officer of any Data Breach issues that are brought to their attention. ➤ Ensure that employees who have responsibility for processing personal data attend the relevant training.
Data Protection Officer	<ul style="list-style-type: none"> ➤ Inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws. ➤ Monitor compliance with the GDPR and other Data Protection laws, including managing internal data protection activities, advise on Data Protection Impact Assessments, train staff and conduct Internal Audits. ➤ Be the first point of contact for Supervisory Authorities and for people whose data is being processed.
All Employees/Volunteers	<ul style="list-style-type: none"> ➤ Take due care to ensure compliance with the Data Protection Policy and Procedure. ➤ Act in a way that protects Individuals and the Council from the adverse impacts of a Data Breach. ➤ Bring matters of concern about potential or actual data breaches to the attention of their Line Manager.

5. Implementation.

- 5.1 The Policy will be supported by a Data Protection Policy Framework.
- 5.2 The Framework gives further guidance in relation to Lawful Processing, Individual Rights, Data Subject Access Requests, Information Sharing, Privacy Impact Assessments, Privacy Notices, and Data Security Breach Notification.

6. Linkages.

- 6.1 The Data Protection Policy will link in to the Council's Access to Information Policy.

7. Review.

- 7.1 The Data Protection Policy will, under normal circumstances, be formally reviewed every three years.
- 7.2 The Policy will also be subject to routine scrutiny and, from time to time, updates and re-issues will be circulated.
- 7.3 The policy will be reviewed sooner in the event of any one or more of the following:
 - A failure or weakness in the policy is highlighted.
 - Changes in legislative requirements.
 - Changes in Government/Council or other directives and requirements