Fermanagh & Omagh
District Council
Comhairle Ceantair
Fhear Manach agus na hÓmaí

Data Protection Policy

and

Procedural Framework

Title:	Data Protection Policy and Procedural Framework (previously Data Protection Procedural Framework)
Version:	2
Directorate/Departmental ownership:	Corporate and Strategic Services
Officer responsible:	Head of Corporate and Strategic Services
Corporate Leadership Team authorised on:	8 November 2024
Policy and Resources Committee authorised on:	11 December 2024
Review date:	November 2027
Location where document is held and referenced:	Policy Register

Work	Date	Version
Created	May 2018	1
Amended	November 2024	2

Contents	
Detail	**Page No**

Fermanagh & Omagh
District Council
Comhairle Ceantair
Fhear Manach agus na hÓmaí

Data Protection Policy

1 Introduction

Fermanagh and Omagh District Council (FODC) needs to collect and use personal data about people with whom it works in order to operate and to carry out its functions. These may include members of the public, current, past and prospective staff, clients, customers and suppliers. In addition, the Council may be required to collect and use personal data in order to comply with legislative requirements.

This personal data must be handled and dealt with properly, regardless of the way in which it is collected, recorded and used. The information may be on paper, in computer records or recorded by other means e.g. CCTV footage.

Good Data Protection practice is not just a matter of legal compliance and ticking the boxes. Data Protection is about taking care of people and respecting their privacy. Poor information security leaves our systems and services at risk, can cause real harm and distress to individuals, and can have a detrimental effect on the reputation and financial position of the Council.

This policy contributes towards FODC's Corporate Plan by supporting effective governance of the Council and supporting our staff to act with integrity, which is one of our core values.

What is Personal Data?

Personal Data: Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
This may include first name; surname; address; telephone numbers; date of birth; age; qualifications; training records; financial information; licensing information; enforcement action and complaint information.

Special Category Data: Special category data is personal data, which the legislation considers sensitive and deserving of extra attention. This includes racial or ethnic origin; religious or other philosophical beliefs; political opinions; trade union membership; physical or mental health or condition; sexual orientation.; offences (including alleged offences); genetic data; biometric data and health data.

2 Aims

The aims of the policy are to:

- Provide assurance to our staff and the public that we seek to protect the information we hold and we use it for legitimate purposes;

- Ensure Council meets the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018);

- Set out the standards expected by the Council in relation to processing of personal data and safeguarding individuals' rights and freedoms; and

- Ensure that all appropriate staff are properly trained, kept fully informed of their obligations under the DPA 2018, and that they are aware of their personal data protection liabilities.

3 Who does this Policy apply to?

The obligations contained in this Policy apply equally to:

- All Council staff, including graduates, placement students, agency workers (where they are employed by FODC),

- Elected Members when working on Council business; (Elected Members are separate data controllers when carrying out electoral ward or constituency duties; those activities are not covered by this policy),

- Partners and other third parties, including contractors, secondees (into the Council) volunteers, agencies, and any other organisation(s) processing personal data on behalf of the Council are bound by the practices established in this policy and the terms of the agreement or contract with the Council, and

- Those working for Fermanagh and Omagh Policing and Community Safety Partnership (PCSP) who are Council staff.

This policy does not apply to staff seconded to other organisations for the period of their secondment. They would be covered by their host organisation's policies.

4 Roles and Responsibilities

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

Group or Individual	Role and Responsibilities
Elected Members	➢ Approve the Data Protection Policy and subsequent amendments. ➢ Attend any relevant training or awareness raising sessions. ➢ Act in accordance with the Policy and the Procedural Framework at all times.
Chief Executive	➢ Embedding Data Protection principles throughout the Council.
Corporate Leadership Team	➢ Allocate resources to enable the Council to meet its responsibilities. ➢ Promote the integration of Data Protection principles into the culture of the Council. ➢ Consider data protection and related issues at CLT meetings, for example on cyber security measures and risks.
Heads of Service	➢ Ensure staff are aware of this policy.

Group or Individual	Role and Responsibilities
	➢ Notify the Data Protection Officer of any issues, such as data breaches, that are brought to their attention. ➢ Ensure that staff who have responsibility for processing personal data attend the relevant training.
Head of Corporate and Strategic Services	➢ Be the senior responsible owner for the Policy and ensure it is updated every three years ➢ Ensure that staff training is made available and updated alongside the Policy ➢ Monitor and report the number and severity of data breaches to CLT in the quarterly information management report.
Data Protection Officer (DPO)	➢ Inform and advise the organisation and its staff about their obligations to comply with the UK GDPR and other data protection laws. ➢ Monitor compliance with the UK 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 the ICO and for people whose data is being processed.
Staff/Volunteers/ Contractors	➢ Take due care to ensure compliance with the Data Protection Policy and Framework. ➢ Attend all available training. ➢ 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 and to the DPO.

5 Implementation

5.1 The Policy will be supported by the Data Protection Procedural Framework.

5.2 The Framework gives further guidance in relation to Lawful Processing, Individual Rights, Subject Access Requests (SAR), Information Sharing, Data Protection Impact Assessments (DPIA), Privacy Notices, Data Breach Notification, Security and CCTV.

6 Related Legislation and Policies

6.1 Related Legislation

The Council must comply with all statutory UK legislation that has links to the UK GDPR and DPA 2018 these include, but are not limited to:

- Human Rights Act 1998
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Common law Duty of Confidence
- Public Records Act (Northern Ireland) 1923
- Regulation of Investigatory Powers Act 2000

- Criminal Justice and Immigration Act 2008
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- Data Protection (Charges and Information) Regulations 2018.
- Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 2002
- The Local Government Act (Northern Ireland) 2014
- The Local Government Act (Northern Ireland) 1972
- Access to Health Records (Northern Ireland) Order 1993

6.2 Related Policies

This policy should be read in conjunction with the following FODC policies:

- Information, Communications and Technology Policy and Procedures for Employees and for Elected Members;
- Disciplinary Policy;
- Access to Information Policy;
- CCTV Protocol;
- Records Management Policy and the Records Retention and Disposal Schedule; and
- Safeguarding Policies (for Children and for Adults at Risk)

7 Review

7.1 The Data Protection Policy will 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.

Fermanagh & Omagh
District Council
Comhairle Ceantair
Fhear Manach agus na hÓmaí

Procedural Framework

1 About the Procedural Framework

The Procedural Framework sets out in more detail how FODC will meet its data protection obligations.

The Framework makes reference to additional sources of information as well as templates and forms that are available to staff to help them to fulfil their data protection obligations, ensure transparency and provide audit trails.

2 Data Protection Principles

FODC must comply with the UK GDPR principles (Article 5) and the DPA 2018 and ensure that personal data is:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject **('lawfulness, fairness and transparency')**.
b) 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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes **('purpose limitation')**.
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed **('data minimisation')**.
d) 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 (**'accuracy'**).
e) 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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (**'storage limitation'**);
f) 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 (**'integrity and confidentiality'**).

Finally, in relation to the points a) – f) above, personal data must be processed in line with the **Accountability** principle[1].

3 Lawful Basis for Processing

FODC must have a lawful basis for processing personal data. We should determine and document our lawful base/s before we begin processing. The FODC privacy notice includes our lawful basis for processing as well as the purposes of the processing.

[1] Article 5 (2) of the GDPR 'The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')'

There are six lawful bases for processing:-

a) **Consent**: the individual has given clear consent for the processing of their personal data for a specific purpose.
b) **Contract**: the processing is necessary for a contract the Council has with an individual or because an individual has asked the Council to take specific steps before entering into a contract.
c) **Legal obligation**: the processing is necessary for the Council to comply with the law (not including contractual obligations).
d) **Vital interests**: the processing is necessary to protect a data subject's life.
e) **Public task**: the processing is necessary for the Council to perform a task in the public interest or for its official functions, and the task or function has a clear basis in law.
f) **Legitimate interests**: the processing is necessary for the Council's 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. (Please note, this does not apply if the processing relates to the Council's statutory obligations.)

When processing special category data, we must have a lawful base/s AND meet one of the specific conditions below (the lawful base and specific condition do not have to be linked):

a) **Explicit consent**: the individual has given explicit consent for the processing of their personal data for a specific purpose.
b) **Employment and Social Security**: processing is necessary for the purposes of carrying out obligations in the fields of employment, social security, and social protection law.
c) **Vital interests**: the processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
d) **Not-for-Profit Bodies:** processing is carried out for the members (or former members of the body or to persons who have regular contact with it in connection with its purposes), and in the course of the legitimate activities of, a foundation, association, or trade union, and not disclosed outside of that body without the consent of the data subjects.
e) **Manifestly Public**: processing relates to personal data which are manifestly made public by the data subject.
f) **Legal Claims:** processing is necessary for the establishment, exercise, or defense of legal claims.
g) **Substantial Public Interest:** processing is necessary for reasons of substantial public interest.
h) **Health or social care:** processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the staff member, medical diagnosis or health and social care.
i) **Public Health:** processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health.
j) **Archiving, research, and statistics:** processing is necessary for archiving purposes in the public interest, scientific, historical, or statistical purposes.

4 Data Subject Rights

Individuals have a number of rights relating to their personal data. These are:

1) The **right to be informed** - individuals have the right to be informed about the collection and use of their personal data.
2) The **right of access** – individuals have the right to obtain confirmation that their personal data is being processed and have access to it (also known as SAR).
3) The **right to rectification** - a right for individuals to have inaccurate personal data rectified or completed if it is incomplete.
4) The **right to erasure** - a right for individuals to have personal data erased (also known as the right to be forgotten).
5) The **right to restrict processing** - individuals have the right to request the restriction or suppression of their personal data.
6) The **right to data portability**- allows individuals to obtain and reuse their personal data for their own purposes across different services.
7) The **right to object** – allows individuals 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.
8) **Rights in relation to automated decision making and profiling** – gives individuals rights when their personal data is used to make decisions by automated means without human involvement.

Making a Subject Access Request

Individuals have the right to access and receive a copy of their personal data, and other supplementary information. This is commonly referred to as a subject access request or 'SAR' (or Data Subject Access Request – DSAR). It may be made in writing, verbally or via social media. However, staff will process requests via the SAR Form (Annex 1). Proof will be required that they are the data subject, or have authorised someone to act on their behalf.

The request should be acknowledged within 3 working days and FODC should respond to a request within one calendar month of receipt. This time limit can be extended by a further two months if the request is complex or where a number of requests are made by an individual. The information should be disclosed securely.

Requesters will receive a copy of all, or part, of the data we hold about them, and an explanation why some data cannot be provided if that is the case. Information will be withheld if it is:-

- Information about another person;
- Information which may prevent the detection of a crime or prosecution of an individual, or which may affect a legal matter such as an enforcement case; and
- Information which it is believed would cause them, or another person, serious physical, mental or emotional harm if shared or disclosed.

A person can ask a third-party representative to act on their behalf when making a SAR, such as, a solicitor, financial advisor, doctor, carer or family member. In this case, the

Council must be satisfied that they have consented to this arrangement so we will ask the representative to demonstrate this.

In cases where data subjects are incapable of understanding or exercising their rights, for instance because they are too young, then SARs may be made by parents or other persons who are legally able to act on behalf of the data subjects.

FODC does not charge a fee to deal with a SAR.

On rare occasions, FODC may refuse to provide information if the request is manifestly unfounded or excessive.

Privacy Notices

The Council will take all reasonable steps to ensure that data is obtained and processed fairly and that individuals are aware of the processing activities which the data will be subject to (this applies to data collected in paper and/or electronic format).

If the Council collects personal data directly from data subjects, it will inform them of the purpose/s for which it intends to process that personal data and the lawful basis for processing it; and contact details of the Data Controller.

In order to do this, the Council will provide a short Privacy Statement (Annex 2) at the point at which data is collected from a data subject.

If the Council receives personal data from a third party, it will provide the data subject with the above information in the first communication with them or as soon as possible thereafter, but no later than one month of receiving the information. This will apply unless there is an applicable legislative exemption.

In addition, the Council has adopted a Privacy Policy Statement (Annex 3) providing information to data subjects on their rights and the Council's practices and procedures.

5 Data Protection Officer

The UK GDPR introduced a duty on public authorities to appoint a Data Protection Officer (DPO).

The DPO assists the Council in:

- creating data protection policies and guidance,
- monitoring compliance with the UK GDPR and other data protection legislation,
- awareness raising and training,
- performing data protection compliance audits,
- informing and advising on data protection obligations,
- providing advice and assistance with completing Data Sharing and Processing Agreements and Data Protection Impact Assessments (DPIAs), and
- acting as a contact point for data subjects and the Information Commissioner's Office (ICO).

The Council will:

- take account of the DPO's advice and the information they provide on data protection obligations.

FODC's DPO is:

- an existing staff member,
- involved in all issues relating to the protection of personal data held by the Council,
- independent in their role as DPO,
- an expert in data protection,
- sufficiently well-resourced to be able to perform their tasks,
- reporting to the highest management level (the Chief Executive),
- not penalised for performing their duties, and
- responsible for ensuring that any other tasks or duties do not result in a conflict of interest with their role as DPO.

FODC's DPO also acts as the DPO for[2] the Fermanagh and Omagh PCSP and FODC animal welfare staff (who are part of a wider regional group).

In order to demonstrate the Council's compliance with data protection laws, the DPO will conduct regular audit inspections of service units and third-party processors. Audits may take a number of forms, including onsite review of processing activities and records, discussions with staff involved in processing activities, and any other action which is, in the opinion of the Data Protection Officer, necessary to ensure that personal data is processed in line with data protection law.

The DPO is easily accessible as a point of contact for staff, individuals and the ICO. FODC has published the contact details of the DPO (dpo@fermanaghomagh.com) and communicated them to the ICO.

The Council's DPO (as at October 2024) is Louise Horner, Head of Corporate and Strategic Services.

Where the DPO investigates a breach, the investigation follows the report in Annex 4.

Registration with the Information Commissioner's Office

The DPA 2018 requires every Data Controller who is processing personal data to register with the ICO unless they are exempt. FODC's Registration Number is ZA089771. The Council pays all fees, relating to its responsibilities as a data controller, as required under section 2 of the Data Protection (Charges and Information) Regulations 2018.

[2] A number of staff working on water quality are contracted to work for FODC, however, their routine activity and work is for the NI Environment Agency and as such, are covered by their data protection policy and would liaise with the NIEA DPO.

6 Personal Data Breaches

The Council interprets a **personal data breach to mean a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed**.

All personal data breaches, either as a result of Council action or those of a third-party acting on behalf of the Council, must be notified to the DPO as soon as possible after the breach has taken place or been identified. The breach notification procedure and breach report form can be found at Annexes 5 and 6.

The aim of the process is to have a standardised management approach throughout the Council in the event of a serious security incident or data breach by having clear policies and procedures in place. Fostering a culture of proactive reporting and logging of incidents will help reduce the number of breaches which often go unreported and unnoticed.

Objectives

The objectives of the process are to ensure that:

1. All data breach incidents are detected, reported, categorised and monitored consistently.
2. Incidents are assessed and responded to appropriately.
3. Action is taken to reduce the impact of disclosure.
4. Mitigation improvements are put in place to prevent recurrence .
5. Serious breaches are reported to the Information Commissioner.
6. Lessons learnt are communicated throughout the Council as appropriate to try to prevent future incidents.

The process relates to all personal and special category data held by the Council regardless of format, and applies to all staff within the Council, including temporary, casual or agency staff and contractors, consultants, suppliers and data processors working for, or on behalf of the Council.

For the purpose of this process, data breaches include both confirmed and suspected incidents. A data breach is the result of an event or series of events where personal data is exposed to unauthorised or inappropriate processing that results in its security being compromised. The extent of damage or potential damage caused will be determined by the volume, sensitivity and exposure.

A Data Breach, which is often the result of human error, includes but is not restricted to, the following:

- Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad/tablet device, or paper record);
- Equipment theft or failure;
- Unauthorised use of, access to, or modification of data or information systems;
- Attempts to gain unauthorised access to information or IT system(s);
- Unauthorised disclosure of sensitive/confidential data;
- Hacking attack where personal data has been lost or compromised;

- Unforeseen circumstances such as a fire or flood resulting in loss or damage to personal data;
- Blagging offences where information is obtained by deception; and
- Verbal breaches e.g. telling people about someone's medical history or criminal convictions without authorisation.

The Council will maintain a Data Breach Register which will contain the following information:

- Details of each data breach, which will include date, time, location, responsible officer, specific details of the information release and details of when the DPO was notified;
- Details of any remedial action taken or action taken to minimise the impact of the data breach;
- Whether the ICO has been notified and details of considerations which informed that decision;
- Whether the data subject has been notified; and
- In the context of the breach, any other information which it is considered necessary to record.

A data breach which is considered, in the opinion of the DPO, to result in a high risk to an individual's rights or freedoms will be reported to the ICO and Chief Executive by the DPO without undue delay and not later than within 72 hours of the breach occurring or the Council becoming aware of it (including weekends).

Circumstances relating to a personal data breach, which was the established fault of a third-party processor or partner in a data sharing arrangement, may, dependent on the terms of that agreement or contract, trigger a review of that arrangement.

7 Data Sharing

The Council will ensure that any data sharing arrangements comply with the principles of the UK GDPR and the DPA 2018, and therefore adopt the ICO's Data Sharing Code of Practice as the basis for its own data sharing arrangements.

The Council will primarily utilise two types of data sharing:

- As part of a systematic and routine process (both internal and external) where personal data is shared on the basis of a lawful processing condition; and
- In exceptional circumstances, such as the need to process information to protect the vital interests of a data subject.

The DPO must be notified and consulted by the relevant Service Area before it enters into any data sharing arrangement to ensure that all relevant matters have been taken into consideration, such as the completion of a Data Protection Impact Assessment.

Internal Sharing

In some circumstances information may be required to be shared internally between Council Services to meet a specified need which differs from the initial processing purpose

of the information. Sections review the lawful basis for processing the data and go back to individual/s to seek consent again if necessary.

Disclosure of personal data to third parties and Elected Members

The Council will take cognisance of Schedule 1, Part 2, Section 24 of the DPA 2018 and the ICO Guidance document 'Disclosure of personal information by local authorities to Councillors' when releasing information to Elected Members. Personal data will only be disclosed to other third parties with the express written permission of the individual to whom the information belongs, unless for one of the reasons in Section 24 sub paragraph 2.

Disclosure of personal data to statutory law enforcement agencies

The DPA 2018 includes exemptions which allow personal data to be disclosed to statutory law enforcement agencies without the consent of the individual who is the subject of the data. In particular, personal data may be released in line with those exemptions detailed within Schedule 2 of the DPA 2018.

Data Sharing Register

The Data Protection Officer will maintain a central register of data sharing arrangements and contracts with third party processors. This will include:

- Service Area/s involved;
- The title of the contract or agreement;
- Processing or sharing agreement;
- Long or short version;
- Name of other party/ies
- A description of the data to be shared or transferred;
- Lawful basis for processing; and
- The date the agreement or contract is effective, terminates and, if applicable, is reviewed.

NB. Personal Data / Special Category Data, in any format, should not be shared with a third-party organisation without a valid agreement in place (e.g. a Data Sharing Agreement (Annexes 7 and 8), a Contract, PSNI Form 81), or the consent of the data subject(s). Personal Data/Special Category Data should not be transferred outside of the UK, without appropriate safeguards. Safeguards and technical measures will be informed by an assessment of the level of protection for the rights and freedoms of the data subjects in relation to the processing activities.

8 Data Protection Impact Assessment & Screening

A Data Protection Impact Assessment (DPIA) is required if the processing of personal data is likely to result in a high risk to individuals. For a new or evolving project/activity, which involves the use of personal data, a screening exercise is needed to identify data protection implications and to determine if a DPIA is necessary. If it is necessary, it must be completed:-

- Before the introduction of a new processing activity or activities (including the introduction of new policies, technologies or operational procedures); or
- Before a change is made to an existing processing activity or activities (including a change to existing policies, technologies or operational procedures).

A DPIA must be completed by the Service Manager, Head of Service or Director responsible for the processing activity, in consultation with the Data Protection Officer.

The DPO should consult with the ICO if the DPIA identifies a high risk and there are no measures to reduce that risk.

A screening exercise and template DPIA are available at Annex 9.

9 Security

The UK GDPR says that personal data shall be: **"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"**.

This means that FODC must have appropriate security to prevent personal data being accidentally or deliberately compromised. Information security includes cybersecurity (the protection of our networks and information systems from attack) but also covers other things like physical and organisational security measures.

Information security is important because it is a legal requirement and demonstrates good data governance in terms of demonstrating FODC's compliance with other aspects of the UK GDPR. Poor information security leaves systems and services at risk and may cause real harm and distress to individuals.

Examples of the harm caused by the loss or abuse of personal data include:

- Identity fraud;
- Fake credit card transactions;
- Targeting of individuals by fraudsters, potentially made more convincing by compromised personal data;
- Witnesses put at risk of physical harm or intimidation;
- Exposure of the addresses of those at risk of domestic violence; and
- Embarrassment and reputational damage to an individual.

The ICO is also required to consider the technical and organisational security measures we had in place when considering an administrative fine for a breach of data protection legislation.

The security principle goes beyond the way information is stored or transmitted. Every aspect of processing of personal data is covered, not just cybersecurity. This means the security measures that are put in place should seek to ensure that the data we hold is accurate and complete, and the data remains accessible and usable.

These are known as ‘confidentiality, integrity and availability’ and under the UK GDPR, they form part of FODC’s obligations.

The UK GDPR does not specifically define the security measures that FODC should have in place. It requires the Council to have a level of security that is ‘appropriate’ to the risks presented by the processing of data.

The first consideration is how valuable, sensitive or confidential it is – as well as the damage or distress that may be caused if the data was compromised. Other considerations include:

- The nature and extent of the Council’s premises and computer systems;
- The number of staff and the extent of their access to personal data; and
- Any personal data held or used by a data processor acting on behalf of the Council.

The Council has a range of ICT Policies and Procedures covering, all Servers, PCs, Mobile Computers, Tablets, Telephony, Smart Phones, Mobile Phones, Digital Cameras, Memory Sticks, any other USB devices, Modems, CDs, DVDs, handheld wireless devices, wireless networking cards, and any other existing or future device that may connect to or access the systems at FODC.

In considering physical controls, each building/facility should consider:

- Quality of doors, locks, lockable storage, alarms, CCTV;
- Controlled access to premises, particularly supervision of visitors and contractors; and
- Secure disposal of paper waste.

Staff should:

- Be familiar with the policy and procedural framework and the quick guide ‘GDPR general guidance and FAQs’

Secure Desk Policy

Desks, workstations, etc should be free from documentation which contains personal data. Documents containing personal data, which are likely to be needed by other members of staff, should be stored in lockable filing cabinets/stores. Documentation containing personal data should not be visible to visitors, members of the public or colleagues who are not authorised to see them.

Secure Screen Policy

FODC staff must lock or secure Council PCs, laptops, iPad, tablets or other electronic devices (e.g. mobile phones) when leaving for long periods and overnight; or when leaving the desk for more than a short period of time, for example at lunchtime. Open documents, containing personal data, should not be visible on screens to visitors, members of the public or colleagues who are not authorised to view them.

10 Miscellaneous issues

Destruction of personal data

Personal data held by the Council should be destroyed in line with the Council's Records Retention and Disposal Schedule. Personal data held on behalf of the Council by a third-party processor should be destroyed in line with the terms of that contract or agreement.

Mailing Lists and Consent

Consent should be refreshed regularly for the personal data of individuals who are on mailing lists or databases (both electronic and postal) on the basis of consent. Lists and databases attached to specific projects should be refreshed or destroyed, as appropriate, at the conclusion of those projects. A template letter requesting consent can be found at Annex 10.

Photographic and video images

When taking images, or using images of individuals who are under 18 years of age or adults who may be vulnerable, consent should be sought from their parent/guardian. Consent may be required, in certain circumstances, from individuals over 18 years of age before photographic or video images of that individual are captured and used.

The following circumstances may not require the written consent of individuals over 18 years of age:

- Where the person is aware that their photograph may be published and that neither the photograph itself nor the context in which it is used could cause any potential harm or distress to that person; and that the person is able to opt out if they wish to do so; and
- Where the individual photographed is unrecognisable, e.g. if they have their back to the camera, or they appear out of focus.

Where photographs are being taken at a public event attended by large crowds within a public area, the consent of all the attendees is not necessary. Large signs are available for display at large scale events to advise of photography and videography. Images must not, however, be used out of context, and there must be no reason to believe that damage or distress could potentially be caused to the people appearing in them.

Criminal offence data

If FODC needs to process data about offenders or suspected offenders in the context of criminal activity; allegations; investigations; and proceedings, a lawful basis for processing and a separate condition for processing this data is required. This needs to be documented to demonstrate compliance and accountability. It also covers a wide range of related security measures, including personal data about penalties; conditions or restrictions placed on an individual as part of the criminal justice process; or civil measures which may lead to a criminal penalty if not adhered to.

Closed Circuit Television (CCTV)

For surveillance systems, FODC considers data protection and privacy issues upfront, from the earliest stages of project planning. A Data Protection Impact Assessment (DPIA) for any processing that is **likely to result in a high risk** to individuals. See also FODC's CCTV Protocol.

11 Key Definitions and Glossary

Biometric Data	Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or fingerprints.
Consent	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Data Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data Erasure	Also known as the Right to be Forgotten, it entitles the data subject to have the data controller erase their personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data.
Data Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Data Protection Impact Assessment	A process used to identify and reduce data protection risks of a project by analysing the personal data that is processed and the policies in place to protect the data.
Data Subject	A natural person whose personal data is processed by a controller or processor.
Encrypted Data	Personal data that is protected through technological measures to ensure that the data is only accessible/readable by those with specified access.
Filing System	Any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.
Personal Data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Privacy by Design	A principle that calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition.
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Profiling	Any form of automated processing of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
Pseudonymisation	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.
Restriction of processing	The marking of stored personal data with the aim of limiting their processing in the future.
Right to be Forgotten	Also known as Data Erasure, it entitles the data subject to have the data controller erase their personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data.
Special Category/ Sensitive Data	Special category data is personal data that needs more protection because it is sensitive.
Subject Access Right	Also known as the Right to Access, it entitles the data subject to have access to any personal data concerning them that a controller may be holding.

DC	Data Controller
DP	Data Processor
DPA 2018	Data Protection Act 2018
DPIA	Data Protection Impact Assessment
FODC	Fermanagh and Omagh District Council
SAR	Subject Access Request
UK GDPR	UK General Data Protection Regulation