



Fermanagh & Omagh  
District Council

Comhairle Ceantair  
Fhear Manach agus na hÓmaí

# Access to Information Policy

July 2016

## **1. Introduction**

- 1.1 The public have a general right of access to the information held by Fermanagh and Omagh District Council and the Council must release information on request, unless a relevant exemption applies. Procedures have been developed to ensure that the Council can respond appropriately to information requests under the Freedom of Information Act 2000, the Environmental Information Regulations 2004, the Data Protection Act, the Regulation of Investigatory Powers Act 2000 and any other legislation that provides a right of access to information.
- 1.2 The Policy sets out the framework within which Fermanagh and Omagh District Council will promote a culture of good practice around the management of Access to Information requests to ensure compliance with our legislative requirements.
- 1.3 The Legislative Framework is set out as Appendix A to this policy.

## **2. Objectives**

The objectives of this Policy are to:

- Promote greater openness and increased transparency of decision-making;
- Build the trust and confidence of the public and stakeholders; and
- Provide clarity on the way in which the Council will meet its duties under access to information legislations, guidance and best practice.

## **3. Commitment to Openness and Transparency**

Fermanagh and Omagh District Council is committed to promoting and developing a culture of openness, transparency and accountability and will:

- Routinely publish information through the Council website and favour prompt disclosure wherever possible;
- Where information is not made available, explain clearly why and apply any exemptions from disclosure consistently and in accordance with legislation;
- Deal with complaints in a positive and fair manner; and
- Operate a fair and efficient appeal system.

## **4. Responsibilities**

- 4.1 The Council will allocate sufficient resources to ensure the effective operation of the Policy.
- 4.2 Overall responsibility for this Policy and the application of it lies with the Chief Executive.
- 4.3 Directors and Heads of Service are responsible for ensuring the compliance of this Policy within their own sections.

- 4.4 The Head of Policy and Strategic Services and Policy Officer are responsible for the distribution of information, training to all appropriate staff and for requests overall.
- 4.5 All relevant staff are responsible for ensuring that requests for information are dealt with in compliance with the Policy, and the attached Procedures.
- 4.6 Any breach of this Policy document will be regarded as a serious matter. Staff who are in breach will be dealt with according to the Council's disciplinary procedures.

## **5. Implementation**

5.1 The Policy will be supplemented by specific guidance:

- Procedure for dealing with requests – Appendix B
- Guidance on Freedom of Information and Environmental Information Regulations – Appendix C
- Guidance on Data Protection requests – Appendix D
- Guidance on Regulation of Investigatory Powers Act requests – Appendix E

5.2 The Policy also links in to the ICT Policies and Procedures.

## **6. Review**

The Access to Information Policy will be reviewed every two years.

However, the policy will be reviewed sooner in the event of any one or more of the following:

- Weakness in the policy is highlighted,
- Weaknesses in hardware and software controls are identified,
- In case of new threat(s) or changed risks,
- Changes in legislative requirements, and/or
- Changes in Government/Council or other directives and requirements.

## Legislative Framework

### 1.1 Introduction

When the Council receives an information request, it will consider the nature of the information requested and, if applicable, identify the statutory access regime under which it will respond to that request.

### 1.2 Freedom of Information Act

The Freedom of Information Act 2000 (FOIA) provides the public with a general right of access to information held by the Council. When a written request for information is made, the Council must provide a response promptly and no later than 20 working days. If the Council holds the information on any record system (including backup systems and off-site storage archives) then the Council must usually provide the requester with the information. Any information in the possession of, or held on behalf of, the Council is potentially disclosable, provided it is held for the purpose and interest of the Council. The Act defines specific exemptions that apply where the Council may not be obliged to release the information.

### 1.3 Data Protection Act

The Data Protection Act 1998 (DPA) requires all organisations which handle personal information to comply with important data protection principles including in relation to privacy and disclosure. The Act also allows people to find out what personal information is held about them by making a Subject Access Request (SAR). This covers information held electronically and in some paper records. The Council should respond to SAR promptly and no later than 40 calendar days.

The Council is a registered data controller and is required to process data in accordance with the eight data protection principles.

### 1.4 Environmental Information Regulations

Some requests for information do not fall under DPA or FOIA but may instead be requests for environmental information. The Environmental Information Regulations 2004 (EIR) give members of the public the right to access environmental information held by public authorities. If the Council receives a request for information held on any of the environmental areas mentioned below, it is normally obliged to provide it promptly and no later than 20 working days. There are a number of exceptions to this rule.

EIR covers (in summary) information on the state of the elements of the environment, such as air, water, soil, land, flora and fauna and diversity and will also include information on genetically modified organisms. In addition, information on emissions and discharges, noise, energy, radiation, waste and other such substances; measures and activities such as policies, plans, agreements; reports, cost benefit and economic analyses are included. The state of human health and safety, contamination of the food chain, cultural sites and built structures

as they may be affected by environmental factors, are also considered to be environmental information.

EIR covers both old and new information, and applies to information recorded in any form, including written, visual, audio and electronic. The Council has an obligation to disclose environmental information in our possession which has been produced or received by us, or if it is stored elsewhere, by another person, on our behalf. This definition is wider than that under FOIA.

### **1.5 Regulation of Investigatory Powers Act**

The Regulation of Investigatory Powers Acts 2000 regulates the powers of public bodies to carry out surveillance and investigation. The Council uses Closed Circuit Television (CCTV) systems at a number of Council owned sites across the District Council area. If the Council receives a request to view or download footage it must be dealt with as any other request for information.

### **1.6 Combined Requests**

If a request for information comprises a combination of personal information relating to the individual requesting the information, environmental information or other information then the Council will separate out the request and deal with each element separately under the DPA, EIR, FOIA and RIPA, as appropriate.



Fermanagh & Omagh  
District Council

Comhairle Ceantair  
Fhear Manach agus na hÓmaí

## **Access to Information Policy**

### **Procedure for Dealing with Requests**

# **1 How requests for information will be managed**

## **1.1 All requests for information will be responded to**

Requests for information will be co-ordinated by the Policy and Strategic Services department assisted by the Personal Assistants of each Directorate.

Where a requester wants to have their request dealt with under the access to information legislative framework, the Council will ensure that this is put in writing. Legally EIR requests can be made verbally, over the phone or in person. Where this does happen, the Council will put it in writing and process the request as a standard information request and, as part of this process, consider whether or not the request should be dealt with under EIR.

All requests for personal information relating to the individual requesting the information, including requests for CCTV footage, will be dealt with under DPA in terms of this policy and will require that the request meets the requirements of being a Subject Access Request and if it does, the requester will be asked to fill in a Subject Access Request form.

Requests for viewing or downloading CCTV footage by the PSNI must include a Form 81 which the PSNI provide themselves.

It is imperative that all staff must check and seek the approval of their line manager/supervisor when necessary, before making any disclosure or release of personal data by letter, fax, telephone, email or other means.

## **1.2 All written requests for information must be logged corporately.**

All written requests for information must be logged corporately. A unique reference number will be allocated to the request and an acknowledgement will be sent to the requester.

## **1.3 Requests for personal information will be treated as Subject Access Requests**

An individual has the right to find out what personal information is held about them by the Council and this is called a 'Subject Access Request' (SAR). However, the requester does not need to call it a subject access request or make reference to the DPA.

If a requester asks for information about another person, that information is exempt under both FOIA and EIR if, among other reasons, it would be a breach of any of the eight data protection principles to release the information.

The Council will treat SARs in the following way: if an individual wishes to make a request to receive information held about them by Fermanagh and Omagh District Council, they will be asked to complete a Subject Access Request form. There are exemptions to the right to receive personal information, for example, personal information in respect of which legal professional privilege could be claimed.

In order to be valid, a SAR must:

- a) be made in writing,
- b) be supported by proof of identity (e.g. driving licence, passport, birth certificate), in order to prevent unauthorised disclosure;
- c) be clear about the information required, (the Council reserves the right to seek clarification from the requester on order to locate the information); and
- d) include a fee of £10 made payable to 'Fermanagh and Omagh District Council'.

The Council will, upon receiving a SAR, log and acknowledge it. The information, once collated, can be sent electronically, by post or collected in person. Under the DPA, the Council must respond within the 40 calendar day time limit by supplying the relevant information in an intelligible form.

#### **1.4 Information held by other authorities**

If Fermanagh and Omagh District Council does not hold the information requested (or part of it), but is aware that another public body does, the relevant contact details will be provided to the requestor.

#### **1.5 Any exemption must be approved corporately before being applied**

Before an exemption is applied to a request and a response made to a requester, the case will be reviewed corporately by the ATI Advisory Panel, which will advise on whether an exemption applies. There are exceptions to this, e.g. if the request is for personal information about another person this is a Data Protection issue and the information may not be released.

#### **1.6 Any vexatious and repeated requests must be dealt with corporately**

The Council is not obliged to comply with vexatious or repeated requests for information. Where the Council considers that a request may be vexatious or repeated, the ATI Advisory Panel will work closely with the service area to review the case and will make a decision, corporately, if the request should be considered vexatious.

The Council will follow the ICO advice and guidance on vexatious and repeated requests. Where a request is considered vexatious or repeated, the requester must be provided with written notice of this.

#### **1.7 Section 29 and 35 Requests**

The Council is allowed to release personal information for crime and taxation purposes under section 29 and for legal proceedings under section 35 of the Data Protection Act 1998. However, before releasing information the Council must be satisfied that there is a valid reason to release the information.

#### **1.8 Exemptions/Exceptions**

Some information will be exempt from disclosure and this will differ, depending on whether it is a FOIA request, an EIR request or a DPA request. It is important; therefore, that there is due consideration and agreement about which legal regime the request falls under before

applying an exemption. Under FOIA there are 23 possible exemptions that could be applied. Some exemptions are absolute and some are qualified.

There is a presumption under EIR that environmental information must be released. The only available grounds for withholding information are set out in a number of exceptions, all of which are subject to a public interest test and must be interpreted restrictively.

### **1.9 Public Interest Test**

In the case of qualified exemptions, the Council must apply the public interest test in considering whether or not to disclose the information. The test is whether in all circumstances of the case, the Council considers the public interest in maintaining the exemption outweighs the public interest in disclosing the information.

### **1.10 Prejudice Test**

There is a prejudice test to be satisfied in the case of many (but not all) qualified exemptions. In order to engage them there must be a likelihood that disclosure would cause prejudice to the interest that the exemption protects.

### **1.11 Time limit for dealing with requests**

There is an exemption in relation to FOIA requests, where the cost of compliance by the Council exceeds the 'appropriate limit'. The appropriate limit is set at £450. The Council can only include identifying, locating, retrieving and extracting (photocopying/printing) the information at a rate of £25 per hour. So the £450 limit equates to 18 hours or just over 2.5 days work.

In the case of FOIA requests, where it is considered that the 'appropriate limit' for dealing with the request may be exceeded then this may be considered by the ATI Advisory Panel. In any instance where the Council engages this exemption, the Council will record, as evidence, why this consideration has been made. When the Council calculates that a request for information will exceed the appropriate limit, the Council will go back to the requester to advise them of this and ask if they would like to narrow down their request in order to bring the scope of the request within the appropriate limit.

### **1.12 All redactions will be explained in the response**

In some cases information will be 'redacted' or obscured before being disclosed, for example the need to protect the identity of individuals. This redaction will be explained in the response.

## **2. How the Council will proactively publish information**

In commitment to being more transparent and open, the Council will increasingly publish information on the public website with a focus on information regularly requested under the FOIA and in accordance with our desire to promote transparency.

The Council is currently working on a Data Management Project which includes an audit, and analysis, of the information the Council holds with a view to making as much information as possible available to the public as Open Data. Open data is all about 'opening up' non-personal data held by the government and making it freely available. This idea is underpinned by the philosophy that data generated or collected by organisations in the public sector should belong to the taxpayers, wherever financially feasible and where releasing it won't violate any laws or rights to privacy (either for the public or government staff).

Open data is information that:

- is free to use for any legal purpose under the Open Government Licence,
- contains no personal data and meets Data Protection Act legislation, and
- is published in a form that makes it easy to manipulate in software like mobile apps.

### **3.0 How the Council will address ATI request complaints**

Fermanagh and Omagh District Council is committed to providing excellent services to the public and responds to complaints as an important part of service delivery. The Council has an internal complaints process through which complaints are considered. The Information Commissioner's Office provides a further stage of appeal, should the complainant not be satisfied with the outcome of the internal investigation.



Fermanagh & Omagh  
District Council

Comhairle Ceantair  
Fhear Manach agus na hÓmaí

## **Access to Information Policy**

# **Guidance on Freedom of Information and Environmental Information Regulations Requests**

## **1 Introduction**

- 1.1 Access to information is principally governed by 2 main legislative provisions under the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR). They both provide rights of access to information publicly held with limited exception. All requests for information should be treated initially as Freedom of Information requests, section 39 of the FOIA exempts environmental information from being dealt with under the Act and provides that it should be dealt with under EIR.
- 1.2 The Council has a duty to provide advice and assistance to the public; a duty to either communicate the information requested, explain why it is not being released or re-direct the requester to another body if we do not hold the information but know who may have it.
- 1.3 The Council has a performance indicator of responding to 90% of requests for information within the legal requirement of 20 working days (40 calendar days for SAR).

## **2 Guidance for staff**

- 2.1 Requests for information are purpose blind, anybody can make a request for any recorded information which they think the Council may hold in any format.
- 2.2 To make a valid FOIA request, it must be in writing, the requester must give their name and postal/email address and must describe the information they are requesting. The Council will accept verbal EIR requests (they will be logged electronically when received) so long as the requester supplies a name and correspondence details and it is clear what information is being requested.
- 2.3 If further information is required to respond to the request, clarification can be sought and the Council does not have to respond until this information is supplied.
- 2.4 The maximum amount the Council can charge for responding to a FOIA request is £450 (equivalent to 18 hours work at £25 per hour), this is for identifying, locating, retrieving and extracting (photocopying/printing) the information. If a request would take over £450 (18 hours of work) to comply with then the Council does not have to respond but will contact the requester to advise of this and assist in reducing the request. Any decision to charge a fee should be authorised by a Director. There is no charging limit for EIR requests. Further advice can be sought from the Policy and Strategic Services section.
- 2.5 Council must respond to FOIA/EIR requests within 20 working days, if clarification is sought or a fee requested, the time for compliance stops when the clarification/fee is sought and does not begin until the clarification/fee is received. If, after 3 months, the clarification/fee is not received the request will be closed, the requester will be contacted to let them know.
- 2.6 The Council does not have to comply with repeated or substantially similar requests from the same person other than at regular intervals, i.e. if someone is submitting the same or

similar requests repeatedly the Council can consider not responding. Further advice can be obtained from the Policy and Strategic Services section.

- 2.7 The Council can refuse to release information requested under FOIA using one, or more, of 23 exemptions (for EIR requests they are referred to as exceptions and there are 14 of them). For FOIA requests there are Qualified and Absolute exemptions. Absolute exemptions are wholly exempt in their application, e.g. information provided in confidence. Qualified exemptions require a public interest test and/or a prejudice test. In the case of qualified exemptions, the Council must apply the public interest test in considering whether or not to disclose the information. The test is whether, in all circumstances of the case, the Council considers the public interest in maintaining the exemption outweighs the public interest in disclosing the information. There is a prejudice test to be satisfied in the case of many (but not all) qualified exemptions. In order to engage them there must be a likelihood that disclosure would cause prejudice to the interest that the exemption protects. EIR exceptions are all subject to a prejudice test. Further advice can be sought from the Policy and Strategic Services section.
- 2.8 If a member of staff wishes to apply an exemption/exception to a request for information, in most cases, the ATI Advisory Panel should be brought together to consider the request. If the Council withholds information requested, fully or partially, a requesters can appeal the decision of the panel. The appeal will be considered by the Chief Executive and if the Chief Executive upholds the panel's decision the requester has a right to appeal/complain to the Information Commissioner's Office.

### **3 Responsibilities**

- 3.1 Directors and Heads of Service are responsible for ensuring compliance within their own sections.
- 3.2 The Head of Policy and Strategic Services and Policy Officer are responsible for the distribution of information and requests, training to all appropriate staff, responding to requests and for monitoring compliance with agreed performance indicators.
- 3.3 Personal Assistants are responsible for ensuring requests within their own sections are forwarded to the relevant staff and are responded to within the appropriate time limit.
- 3.4 The ATI Advisory Panel is responsible for agreeing exemptions/exceptions, where applicable. The Panel consists of the Council's Legal Advisor, the Head of Policy and Strategic Services, the Policy Officer and one senior member of staff from each Directorate.
- 3.5 All relevant staff are responsible for ensuring that requests for information are dealt with in compliance with the policy and procedures.



Fermanagh & Omagh  
District Council

Comhairle Ceantair  
Fhear Manach agus na hÓmaí

## **Access to Information Policy**

### **Guidance on Data Protection Requests**

## **1. Introduction**

If it is determined that the information requested is personal, where the applicant is the subject of the information, access to the information will be dealt with as a Subject Access Request under the Data Protection Act 1998. Unless the information requested is CCTV footage, in which case it will be dealt with under RIPA, see Appendix D.

## **2 Guidance for staff**

2.1 There are eight data protection principles in the Data Protection Act 1998:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless.
  - (a) at least one of the conditions in Schedule 2 is met, and
  - (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

2.2 It is essential that full compliance with the Act is addressed and each staff member has a duty to maintain the integrity of the information and the confidence of the public who have an expectation their personal information is in safe hands. Staff must abide by the following obligations:

- Ensure proper care is taken when gathering, using or disclosing any personal data where it is necessary to meet your departmental functions;
- Take all necessary steps to keep personal information secure and only use it for the purposes intended;
- Personal comments and remarks on manual files or electronic records (including emails) must be appropriate and professional;
- Ensure the personal data recorded is accurate, clear and adequate;
- Avoid accidental unauthorised disclosure by fax, voice, email or other means by double checking;

- Keep personal data confidential and do not disclose it to any other person unless you are authorised to do so (if in doubt ask your line manager);
- Ensure that any electronic data files or paper printouts containing personal data are disposed of safely and not removed from council premises without appropriate security measures or left in an unsecure area;
- Keep system passwords safe. Change regularly and do not disclose them to anyone;
- Comply with this and other related policies e.g. Records Management Policy, ICT Policy and Procedures; and
- Attend DPA Training, which is mandatory

- 2.3 Requests for information under the Data Protection Act 1998 are similar to FOIA requests; anybody can make a request for any recorded information which they think the Council may hold on them.
- 2.4 If it is clear when a request is received that the information being requested is personal to the requester the request should be logged as normal and a SAR form emailed/posted to them.
- 2.5 Council must respond to SAR within 40 calendar days and can request a fee of £10 to identify, locate, retrieve and extract (photocopying/printing) the information.
- 2.6 If a fee is requested, the time for compliance stops when the fee is sought and does not begin until the fee is received. If, after 3 months, the fee is not received the request will be closed, the requester will be contacted to let them know.
- 2.7 There are exemptions to disclosing personal information, eg the data is, or is likely to become, part of a criminal investigation; they work along the lines of the data protection principles. For further information, contact the Policy and Strategic Services section.

### **3. Responsibilities**

- 3.1 All SAR forms should be forwarded to the Policy and Strategic Services section.
- 3.2 Directors and Heads of Service are responsible for ensuring compliance within their own sections.
- 3.3 The Head of Policy and Strategic Services and Policy Officer are responsible for dealing with SARs, the distribution of information, training to all appropriate staff and for compliance with the Data Protection Act.
- 3.4 All staff are responsible for ensuring that any personal data is processed in a lawful manner.

### **4. Loss of Data**

Any loss of data containing personal information **must be reported immediately** to the Policy and Strategic Services Section.



Fermanagh & Omagh  
District Council

Comhairle Ceantair  
Fhear Manach agus na hÓmaí

## **Access to Information Policy**

### **Guidance on Regulation of Investigatory Powers Act Requests (Requests to view or download CCTV footage)**

## **1. Introduction**

CCTV systems are installed in Council premises for a number of reasons:

- To increase the safety of staff, customers and the general public in and around Council premises,
- To prevent, detect and investigate crime/anti-social behaviour,
- To assist with the apprehension and prosecution of offenders, and
- To assist with insurance claims, health and safety investigations and the overall management and supervision of Council buildings.

Images can be shared with other organisations for the purpose of law enforcement, investigation of incidents/claims or to comply with subject access requests. All disclosures will be in compliance with the Data Protection Act 1998.

It is important to note that having the equipment is not essential, it is the purpose that is vital, equipment should not be installed or kept just because it can be, it should only be placed where there is a purpose. Article 8 of the Human Rights Act states that everyone has a right to respect for private and family life:

1. Everyone has the right to respect for their private and family life, their home and their correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

## **2. Guidance for staff**

2.1 There are 12 guiding principles in the CCTV Code of Practice:

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the

disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
  9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
  10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
  11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.
  12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.
- 2.2 Tampering with or misusing CCTV equipment or images is regarded as misconduct and will lead to disciplinary action, which may result in dismissal or criminal prosecution.
  - 2.3 Any employee who has involvement with CCTV equipment, in particular the monitoring and downloading of images, should be aware that they could be asked to attend court by the Public Prosecution Service if a case using Council CCTV images is brought to court.
  - 2.4 If you receive a request to view or download CCTV footage you should always contact the Policy and Strategic Services section first. There are exceptions which appropriate staff will be made aware of.

### **3. Responsibilities**

- 3.1 The Policy and Strategic Services section has overall responsibility for dealing with requests to view/download CCTV footage.
- 3.2 The Operations and Estates section has overall responsibility for the CCTV systems/equipment and maintenance of systems/equipment.
- 3.3 Day to day management of the CCTV systems lies with ICT or designated managers. ICT will train designated managers to operate equipment as necessary. Where managers have been given responsibility, ICT should only be contacted for queries and problems with equipment.