Access to Information Policy

Title
Newry, Mourne and Down District Council's (NMDDC) Access to Information (ATI) Policy.

Reference CS28

Statement
NMDDC endorses the ATI Policy as a framework for the Council's compliance with and implementation of the Freedom of Information Act (FOIA) 2000, Environmental Information Regulations (EIR) 2004, Data Protection Act (DPA) 2018 and UK General Data Protection Regulation (UK GDPR).

Aim
The aim of the ATI Policy is to ensure NMDDC's compliance with and consistent application of the FOI, EIR, DPA and UK GDPR. NMDDC is committed to providing sufficient resources and appropriate training to ensure the Council achieves this objective. Council will work with the Information Commissioner's Office (ICO) to achieve the highest possible information governance standards.

Scope
NMDDC recognises the right of individuals to access Council information in accordance with the terms of the FOIA, EIR, DPA and UK GDPR.

The ATI Policy applies to:

- All recorded information which NMDDC holds including (but not limited to) any information which is created, received and maintained by Council Officers and Elected Members on behalf of the Council. The FOI, EIR, DPA and UK GDPR are fully retrospective so any past records held by the Council are covered by the legislation;

- The FOIA and EIR will apply to any recorded information which any other entity holds on behalf of the Council; and

- Personal data which Council holds in its capacity as a 'Controller' and/or 'Processor'. Where an entity processes information on behalf of Council as the 'Controller', Council will ensure that the matter of who responds to subject access requests is addressed.

All Council Officers and Elected Members are responsible for complying with the terms of the FOI, EIR, DPA and UK GDPR. All Officers and Members are also expected to comply with the Council's ATI Policy and Procedures in relation to FOI, EIR, DPA and UK GDPR.

Non-compliance with the legislation and the Council's ATI Policy & Procedures may result in the Council breaching its' legal obligations under the legislation. This, in turn, may result in NMDDC being the subject of formal or informal action by the Information Commissioner's Office (ICO).

Related Policies / Legislation
NMDDC's Records Management Policy and Procedure
NMDDC's IT Policies & Procedures

NMDDC's Publication Scheme
NMDDC's Retention & Disposal Schedule
NMDDC's Privacy Notice
NMDDC's Customer Service Charter

Definitions
The "Information Commissioner's Office" means the independent authority set up to uphold information rights in the public interest.

Policy Owner
Assistant Director Corporate Services (Administration)

Contact Details
Assistant Director Corporate Services (Administration)
Head of Compliance

CMT Authorised on	**1 June 2023 (via email)**
SMT Authorised on	**6 June 2023**
Strategy Policy and Resources Committee Authorised on	**15 June 2023**
Council Authorised on	**3 July 2023**
Policy Effective Date	**11 July 2023**
Policy Review Date	**11 July 2027** ***(4 years as per equality scheme commitment 4.31)***

Procedures
The ATI Procedures attached hereto must be adhered to in the delivery of this Policy.

Equality Impact Assessment
This Policy has been assessed on 26 May 2023 under NMDDC's Equality Impact Assessment process and has been screened out as having no impact on any of the groups designated in Section 75 of the Northern Ireland Act 1998.

Rural Impact Assessment
This Policy has been assessed on 26 May 2023 under NMDDC's Rural Impact Assessment process and has been screened out as having no impact on the Rural Needs Act (Northern Ireland) 2016.

Access to Information Procedure

Procedure Overview

This Procedure outlines Newry, Mourne and Down District Council's (NMDDC) framework for:

1. Compliance (Section 1) of the Freedom of Information Act (FOIA) 2000, Environmental Information Regulations (EIR) 2004, Data Protection Act (DPA) 2018 and UK General Data Protection Regulation (UK GDPR) 2018; and

2. Implementation (Section 2) for the above pieces of legislation.

Aim

The aim of the procedure is to ensure NMDDC's compliance with and consistent application of the FOI, EIR, DPA and UK GDPR. NMDDC is committed to providing sufficient resources and appropriate training to ensure the Council achieves this objective. Council will work with the Information Commissioner's Office (ICO) to achieve the highest possible information governance standards.

Scope

The procedure brings together a series of legislation (FOI/EIR/DPA/UK GDPR) providing individuals with the right to access information held by Council. It applies to everyone processing recorded data held by Council (including but not limited to, staff, elected Members, other public representatives, contractors, agents and all third party data processors).

CONTENTS	**PAGE**
Section 1: Compliance • FOIA • EIR • DPA/UK GDPR *Introduction* *What is covered by the legislation* *Time limits* *Charging* *Exemptions / Exceptions*	 2 5 7
Section 2: Implementation • Access to Information Procedure • Roles & Responsibilities • Training • Monitoring & Review	 21 28 31 31

Freedom of Information Act (2000)

Introduction

The FOIA gives the public the legal right to access information held by public authorities (subject to a number of legal exemptions).

The aim of the FOIA is to promote a culture of openness and accountability in local Government and to facilitate a better understanding of how we, as a Council, conduct our duties, make decisions and spend public money.

What is covered by the legislation

The FOIA applies to all recorded information which the Council holds including (but not limited to) any information which is created, received and maintained by Council Officers and Elected Members on behalf of the Council. The FOIA is fully retrospective, so any past records held by the Council are covered by the legislation.

Time limits

Any person who makes a request to the Council for information will be informed within 20 working days from the date of receipt of their request whether the Council holds the information requested. If the Council holds the information requested the requester will be provided with the information within 20 working days of the date of receipt of the request (subject to legal exemptions). Please note that 20 working days is the statutory maximum period within which public bodies must respond to a request. The Council will, however, endeavour to provide information to requesters in as short a timeframe as possible. Please also note that the statutory period of 20 working days may be extended for a further 20 working days in limited circumstances and the requester will be advised if this is the case.

Council may request clarification in relation to a request for information. Clarification may be sought in order to assist the Council in identifying and locating information relevant to a request. Where the Council requires clarification to be provided by a requester the Council will inform the requester of this as soon as reasonably possible following receipt of the request. Once clarification is received, Council will respond within 20 working days.

Where the Council does not hold the information being requested but the Council is aware that another organisation may hold the information the Council will advise the requester to contact that organisation and, where possible, will provide contact details for that organisation.

Charging

The Council may refuse a request where the cost to the Council of locating, retrieving and extracting the requested information would exceed the appropriate time and cost limits set by the FOIA. These limits are currently set at £450 or 18 hours of a Council Officer's time at £25 per person per hour. Where this amount will be exceeded the Council will inform the

requester of this and may refuse the request or issue a Fees Notice to the requester specifying the fee payable. Where a Fees Notice is issued the statutory period of 20 working days for dealing with the request will be suspended until payment of the Fee has been received by the Council. The requester will be given a period of 3 months within which to make payment of the Fee. If the Fee is not received within this period, the Council will no longer proceed with the request.

Exemptions
Council may refuse to provide information where it believes the information is subject to one or more of the legal exemptions prescribed under the FOIA.

Some exemptions are absolute and if invoked there is no obligation on the Council to consider the request for information further. However, most of the exemptions under the Act are qualified exemptions and are subject to the Public Interest Test. The Public Interest Test is the test applied to information to determine if the public interest in disclosing the information is greater than the public interest in applying an exemption and not disclosing the information. The Council will apply the Public Interest Test in all cases where qualified exemptions apply.

Where a request for information is refused the Council will, in most cases, confirm the fact that the Council holds the information and will provide the requester with details of the legal exemption under which the Council is refusing to provide the information. The Council will also provide details of the reason that the exemption has been applied to the information in question. However, in some cases, the FOIA recognises that it would not be appropriate to even confirm or deny whether the Council holds certain information. Where this is the case the Council will, in accordance with Section 17 of the legislation, issue a Refusal Notice stating the fact of refusal, the exemption being used and the reason why the exemption applies. The list of exemptions are as follows:

Absolute exemptions	Qualified exemptions subject to PIT
Information Accessible By Other Means (Section 21) Information Supplied by, or Relating to, Bodies Dealing with Security Matters (Section 23) Court Records (Section 32) Parliamentary Privilege (Section 34) Personal Information (Section 40) Information provided in Confidence (Section 41) Prohibitions on Disclosure (Section 44)	Information Intended For Future Publication (Section 22) National Security (Section 24) Certificates under ss. 23 and 24: Supplemental Provisions (Section 25) Defence (Section 26) International Relations (Section 27) Relations within the United Kingdom (Section 28) The Economy (Section 29) Investigations & Proceedings Conducted by Public Authorities (Section 30) Law Enforcement (Section 31) Audit Functions (Section 33) Formulation of Government Policy (Section 35) Communications with Her Majesty etc & Honours (Section 37) Health & Safety (Section 38) Environmental Information (Section 39) Legal Professional Privilege (Section 42) Commercial Interests (Section 43)

Environmental Information Regulations (2004)

Introduction

The EIR gives certain rights of access to Environmental Information to the general public.

The aim behind the law is that giving the public access to environmental information will encourage greater awareness of issues that affect the environment. Greater awareness helps increase public participation in decision-making; it makes public bodies more accountable and transparent and it builds public confidence and trust in them.

What is covered by the legislation

Any information in written, visual, aural, electronic or any other material form on:

> (a) the state of the elements of the environment, such as air and atmosphere, water, soil, land, landscape and natural sites including wetlands, coastal and marine areas, biological diversity and its components, including genetically modified organisms, and the interaction among these elements;
>
> (b) factors, such as substances, energy, noise, radiation or waste, including radioactive waste, emissions, discharges and other releases into the environment, affecting or likely to affect the elements of the environment referred to in (a);
>
> (c) measures (including administrative measures), such as policies, legislation, plans, programmes, environmental agreements, and activities affecting or likely to affect the elements and factors referred to in (a) and (b) as well as measures or activities designed to protect those elements;
>
> (d) reports on the implementation of environmental legislation;
>
> (e) cost-benefit and other economic analyses and assumptions used within the framework of the measures and activities referred to in (c); and
>
> (f) the state of human health and safety, including the contamination of the food chain, where relevant, conditions of human life, cultural sites and built structures in as much as they are or may be affected by the state of the elements of the environment referred to in (a) or, through those elements, by any of the matters referred to in (b) and (c)

Time limits

Requests for information must be responded to within 20 working days. The 20 day time limit can be extended to 40 working days if the complexity and volume of the information requested means that the 20 working days deadline cannot be complied with. Unlike FOIA, there is no provision to further extend the time limit for cases where the public interest has to be balanced.

Council is required to comply with all requests for information as soon as possible and we must not delay responding until the end of the 20 working day period under Regulation 5(2)(b) if the information could reasonably have been provided earlier. Council must aim to make all decisions as soon as possible and in any case within 20 working days, including in cases where a public authority needs to consider where the public interest lies. However, it is recognised there will be some instances where, because of the complexity and volume of the information requested it will not be possible to deal with an application within 20 working days. In such cases Council will inform the requester of this as soon as possible and within 20 working days, and will advise the requester when they will receive the information and the reasons for the delay.

Charging

The EIR does not require charges to be made but Council has discretion to make a reasonable charge for environmental information. However, if Council is providing access to a public register, or if the requester examines the information at Council offices, access to the information shall be free of charge. When making a charge, whether for information that is proactively disseminated or provided on request, the charge will not exceed the cost of producing the information.

A schedule of charges will be made available (including, e.g. a price list for publications, or the charge per unit of work which will be incurred to meet a request) when Council proposes to make a charge. When an advance payment is required, the requester will be notified and Council will invite the requester to say whether they wish to proceed with the request, or part of it, or whether the request may be met in some other way (for example, by visiting the offices to inspect the information or by making use of more easily identifiable data). Where advance payment is required the case will remain active for 3 months until payment is received. When a fee payment is received Council will release the information promptly and within 20 working days.

Exceptions

Under the EIR, there is a presumption in favour of disclosure. Council will conduct a public interest test if there are compelling and substantive reasons to withhold it. Below is a list of exceptions most relevant to the Council. For a complete list of exceptions consult the EIR exceptions[1]:

Regulation:
12(3) – Personal Data
12(4) – Type and/or amount of information
12(5)(b) – Adversely affect justice or disciplinary procedures
12(5)(c) – Intellectual Property Rights
12(5)(d) – Confidentiality of proceedings
12(5)(e) – Commercial Interest
12(5)(f) – Voluntary Information
12(5)(g) – Protection of the Environment
13 – Third party personal data
**Note: 12(5)(d-g) may not be used for information concerning emissions*

[1] EIR exceptions: http://www.legislation.gov.uk/uksi/2004/3391/part/3/made

DATA PROTECTION ACT (2018) /
GENERAL DATA PROTECTION REGULATION (2018)

Introduction

The DPA and UK GDPR are two pieces of legislation which establish a framework of rights and duties designed to safeguard personal data. The UK GDPR applies to all EU Member States. The DPA sets out specific provisions applicable to the UK. The UK GDPR and the DPA must therefore be read together.

Data protection is the fair and proper use of information about people. It is part of the fundamental right to privacy – but on a more practical level, it is about building trust between people and organisations. It is about treating people fairly and openly, recognising their right to have control over their own identity and their interactions with others, and striking a balance with the wider interests of society.

In order to carry out Council business Council collects and uses information about individuals. This may include information on members of the public, customers, suppliers, employees (past and current) and all others with whom the Council communicates.

What is covered by the legislation

- Personal data and special category data

Article 4(1) of the UK GDPR advises that 'personal data' means 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;

Special category data is personal data which the UK GDPR says is more sensitive, and so needs more protection. This is particularly so as the loss, theft or mishandling of this category of information is likely to be of a greater detriment to the individual than the loss, theft etc of other categories of personal data. In order to lawfully process special category data, Council must identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9.

The table below sets out personal data and special category data:

Personal Data (Article 4 UK GDPR)	**Special Category Data** (Article 9 UK GDPR)
• Name • Identification number • Location data • An online identifier • Physical • Physiological • Genetic • Mental • Economic • Cultural • Social factors	• Race • Ethnic Origin • Politics • Religion • Trade Union Membership • Genetics • Biometrics • Health • Sex Life or Sexual Orientation

Article 4 of the UK GDPR sets out the main definitions:

- Processing

(2) 'processing' means 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;

- Controller

(7) 'controller' means 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

- Processor

(8) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

Information Commissioner's Office (ICO)
The ICO means the independent authority set up to regulate and oversee the implementation of DPA/UK GDPR (and FOIA/EIR).

Data Protection Principles
Article 5 of the UK GDPR establishes seven key principles. The principles are in **bold** text below. ICO clarification[2] for each principle has been adopted to support Council compliance.

Article 5 (1) requires that personal data shall be:

> **(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');**

Council must have a valid lawful basis in order to process personal data. There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on Council's purpose and relationship with the individual[3].

Most lawful bases require that processing is 'necessary' for a specific purpose. If Council can reasonably achieve the same purpose without the processing, Council will not have a lawful basis.

Council must determine the lawful basis before beginning processing, and should document it.

The lawful bases for processing are set out in Article 6 of the UK GDPR. At least one of these must apply whenever processing personal data:

(a) Consent: the individual has given clear consent for Council to process their personal data for a specific purpose. However, if relying on consent, the consent can be withdrawn at any time. Where an individual is 'required' to provide information, you should not use consent as a lawful basis. Consent must be freely given and cannot be so given where the data subject is under an obligation to provide their personal information.
(b) Contract: the processing is necessary for a contract Council has with the individual, or because they have asked Council to take specific steps before entering into a contract.
(c) Legal obligation: the processing is necessary for Council to comply with the law (not including contractual obligations).
(d) Vital interests: the processing is necessary to protect someone's life.
(e) Public task: the processing is necessary for Council to perform a task in the public interest or for Council's official functions, and the task or function has a clear basis in law.
(f) Legitimate interests: the processing is necessary for 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. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Processing of personal data must always be fair as well as lawful. If any aspect of Council's processing is unfair Council will be in breach of this principle. Fairness means that Council should only handle personal data in ways that people would reasonably expect and not use

[2] Principles - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-UK GDPR/principles/
[3] Lawful bases for processing - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-UK GDPR/lawful-basis-for-processing/

it in ways that have unjustified adverse effects on them. Personal data may sometimes be used in a way that negatively affects an individual without this necessarily being unfair, e.g. processing personal data to impose a fine. What matters is whether or not such detriment is justified.

Transparent processing is about being clear, open and honest with people from the start about who Council is, and how and why it uses their personal data. Council must ensure that it tells individuals about its processing in a way that is easily accessible and easy to understand. Council must use clear and plain language.

(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');

Council will be clear about what it's purposes for processing personal data are. It will record its purposes as part of its documentation obligations and specify them in its privacy information for individuals.

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

Council will ensure the personal data it is processing is: adequate – sufficient to properly fulfil it's stated purpose; relevant – has a rational link to that purpose; and limited to what is necessary – Council will not hold more than it needs for that purpose.

(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');

Council will take all reasonable steps to ensure the personal data it holds is not incorrect or misleading as to any matter of fact. Personal data will be kept updated and if it discovers it is incorrect or misleading. Council will take reasonable steps to correct or erase it as soon as possible. Council will also carefully consider any challenges to the accuracy of personal data.

(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 individuals ('storage limitation');

Council will not keep personal data for longer than is needed. It will create, maintain and regularly review its Retention and Disposal Schedule. Council will also carefully consider any challenges to the retention of personal data.

(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').

Council will ensure that there are appropriate security measures in place to protect the personal data it holds. In addition to the technical security measures set out under Article 32 of the UK GDPR and Council's internal IT Policy and Procedure, the below bullet points are specific requirements that should be adhered to. This is not an exhaustive list and anyone handling personal data on behalf of Council must take all steps necessary to protect personal data and keep it secure at all times.

- **Physical Security of Personal Data:**

Physical security measures should be in place to protect personal data. This includes locking doors, securing filing cabinets containing personal information, protecting premises with alarms, security lighting and CCTV cameras (subject to DPIA, p16) and using confidential waste bins

Each Department must make sure that it knows and holds a record of what personal data it holds and how and where it is stored. When confidential and sensitive personal data is being sent via post the information should be checked by another member of staff before being sent to ensure it is being posted to the correct recipient. In addition, Officers should 'double bag' information being sent where the information contains sensitive personal data or personal data of a confidential nature. Double bagging works by putting the personal data in an inner envelope which marks the material as confidential and has a postal return address. The inner envelope acts as a second barrier to the information being opened by the wrong recipient accidentally or otherwise.

When printing personal data all personal data sent to printers should be collected immediately and either stored securely or disposed of appropriately. Personal data should not be left on printers, photocopiers, fax machines etc.

- **Clear Desk Policy:**

As a general rule personal data should never be left unattended on desks or in meeting rooms etc. The Council will operate a Clear Desk Policy. This will reduce the risk of unauthorised access to, loss of or damage to personal data. It will also ensure that all personal data and confidential information held by the Council is held securely and adequately protected.

The Clear Desk Policy means that at the end of each day it is the responsibility of individual Officer's to clear their desk of all documents that contain any personal data or confidential information. This information must be stored safely and securely (for example, in a locked office, locked filing room or filing cabinet etc).

- **Electronically held Personal Data:**

Please refer to Council's IT policies and procedures saved on the R drive under the 'policies and procedures' folder.

- **Access to Records containing Personal Data:**

Access to paper and electronic records containing personal data must be restricted. Line Managers must ensure that Officers with responsibility for and access to personal data are properly supervised. It is essential that all staff members and Councillors only access records which they have authority to access and which it is necessary for them to access in the course of their work as Council employees / representatives. Any employee / Councillors finding that they have access to data which they are not authorised to use must report this to their Line Manager so that the access can be removed. In the case of Councillors they should report this to the Head of Compliance. Any employee / Councillor with access to data which is no longer relevant to or necessary for their work must ask for the access to be removed. Any employee / Councillor who is aware that unauthorised access is taking place must report this to their Line Manager as soon as they become aware of it. In the case of Councillors they should report this to the Head of Compliance.

Employees should ensure:

- ✓ The 'Leavers' procedure under Council's IT procedure is completed for 'movers' or 'leavers' which includes employees on long term leave; and
- ✓ Refer to Council's IT procedure when seeking additional access to user accounts.

- **Sharing personal data**

Personal data should only be shared internally and disclosed to external third parties (other than the individual who is the subject of the data) where the sharing is compatible with the DPA/UK GDPR.

When sharing personal data internally within the Council, all staff members and Councillors should ensure that the sharing complies with the DPA and the UK GDPR. Sharing personal data across departments without having a lawful basis potentially risks breaching the UK GDPR.

Given Council's obligation to only use personal data for the purpose for which it was collected, all staff members and Councillors should consider dealing with any internal request for information as you would an external request by:

- Complying with the principles set out under Article 5(1) of the UK GDPR (p9 above),
- Ensure you have a lawful basis for sharing under Article 6(1) (p9 above);
- Where the personal data falls within the remit of Article 9(1) (special category data, p8 above), that you have a further reason for the processing under Article 9(2)[4]; and
- Documenting your reasons to share personal data.

Where there is no lawful basis for sharing the information, then it should not be shared.

Council's Corporate Privacy Notice, available on the website, sets out some instances which may require Council to share personal data, for example, for police investigations.

[4] UK GDPR Article 9: https://www.legislation.gov.uk/eur/2016/679/article/9

When personal information is shared Officers should advise the recipient of the purpose for which the information is being provided. Officers should also state that the information should only be used for that purpose and, depending on the nature of the information, Officers may want to restrict the onward sharing of the information by advising that the information should not be disclosed to third parties. Officers should seek assurances from the recipient on how long the personal data will be held for and an assurance that the data will be securely disposed of.

Article 5(2) of the UK GDPR adds that:

> **The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').**[5]

The accountability principle requires Council to take responsibility for what we do with personal data and how we comply with the other principles. Council will have appropriate measures and records in place to be able to demonstrate compliance. The Compliance Team is responsible for implementing this area of work however all employees are required to support the Compliance Team when contacted. Some measures are set out below:

Privacy Notices
When collecting personal data the Council will inform individuals why their personal data is being collected and will be open and honest as to how they intend to use it. The Council will not deceive or mislead any individual when obtaining their personal data. The Council will use people's personal data in ways that they would reasonably expect and will make sure not to do anything unlawful with the data.

All individuals collecting personal data (in any capacity) on behalf of Council must ensure that individuals are fully informed. A "Privacy Notice" must be provided to all individuals from whom the Council collects personal data.

What is a Privacy Notice?
A Privacy Notice is a Notice to let individuals know how Council will use their personal information. This will be different for each case in which personal data is collected. This Notice should be clearly communicated to individuals and should be visible on all Application Forms etc so that the Data Subject is fully aware of the intended uses of their personal information.

"Privacy Notices" should tell people:-

- ✓ The name and contact details of Council.
- ✓ The contact details of its Data Protection Officer - Head of Compliance.
- ✓ The purposes of the processing.
- ✓ The lawful basis for the processing.
    - The legitimate interests for the processing (if applicable).
- ✓ The categories of personal data obtained (if the personal data is not obtained from the individual it relates to).
- ✓ The recipients or categories of recipients of the personal data.

[5] What are the principles - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-UK GDPR/principles/

    - The details of transfers of the personal data to any third countries or international organisations (if applicable).
- ✓ The retention periods for the personal data.
- ✓ The rights available to individuals in respect of the processing.
    - The right to withdraw consent (if applicable).
- ✓ The right to lodge a complaint with a supervisory authority.
- ✓ The source of the personal data (if the personal data is not obtained from the individual it relates to).
    - The details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to).
    - The details of the existence of automated decision-making, including profiling (if applicable).

It is the responsibility of all Officers collecting personal data on behalf of Council to ensure that the appropriate Privacy Notices are provided. Sample Privacy Notices are available from the Council's Compliance Team. Council's Corporate Privacy Notice is available on the Council website.

When collecting personal data via the telephone or face to face the above information should be made clear to the data subject before any processing of their personal data takes place.

Council can use the information collected for a purpose other than the purpose for which it was originally collected, only if the new purpose is compatible with the original purpose[6]. Officers should not collect information unless Council need's to; if information is 'optional' Officers need to reassess whether it is needed at all.

Audit of Information
Council will conduct and regularly review Information Audits to support awareness of Council's data processing activities. The information gathered will be used to support compliance with UK GDPR Principle 7 as well as Business Planning.

Data Protection Impact Assessments
A Data Protection Impact Assessment (DPIA) is a process to help identify and minimise the data protection risks of a project, similar to equality and rural proofing screening. Council will conduct DPIA's for processing that is likely to result in a high risk to individuals and any other major project which requires the processing of personal data.

Data Sharing Agreements
When Council engages another organisation to process personal information on its behalf Council must make sure that the Data Processor enters into a Data Sharing Agreement (DSA) confirming their commitment to process personal data on behalf of Council in accordance with Data Protection legislation. It is the responsibility of all Officers engaging Data Processors to ensure that this Agreement is signed and enforced. Sample Agreements can be obtained by contacting the Compliance Team.

[6] Purpose limitation:- https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-UK GDPR/principles/purpose-limitation/

CCTV (which includes any audio and/or video surveillance/recording device*)
*Recording device means a device capable of electronically or mechanically storing, accessing, or transmitting sounds or images. The term encompasses, among other things, a computer of any size, including a tablet, a notebook, and a laptop; a smart phone, a cell phone or other wireless phone; a camera and other audio or video recording devices; a personal digital assistant (PDA); and any similar devices[7].

Council operates a number of CCTV Cameras at various Council premises throughout the district. The purpose of the cameras is as follows:-

- Protecting areas and premises used by Council staff and the public;
- Deterring and detecting crime and anti-social behaviour;
- Assisting in the identification of offenders leading to their arrest and successful prosecution or other appropriate action;
- Reducing violent or aggressive behaviour towards staff;
- Reducing fear of crime, anti-social behaviour and aggression;
- Protecting Council property and assets;
- Maintaining and enhancing the commercial viability of the District and encouraging continued investment
- Assisting in staff disciplinary, grievance, formal complaints and Health and Safety Investigations.

The systems will not be used for any other purpose than those set out in this document without Council approval, and, where appropriate, notification to staff and following consultation with the Trade Unions. Any novel or non-standard use of the CCTV cameras will require the approval of the Council.

Recording devices will not be used to monitor the progress of staff or individuals in the ordinary course of lawful business in the area under surveillance. Nor are employees permitted to use recording devices to observe staff working practices or time keeping or to assist them in the day-to-day management of staff.

Individuals will only be monitored if there is reasonable cause to suspect a criminal offence or serious breach of discipline, potentially amounting to misconduct has been, or may be, about to be committed and this will only be permitted when authorized and may require authorisation. Officers should consult the Compliance Team before any such action is taken.

Each service operating CCTV cameras must establish who is responsible for the Camera and the images recorded by the Camera. That Officer will be responsible for the implementation of the good practice guidelines set out below:

A CCTV system should not be in use unless Council can demonstrate compliance with all of the below:

<u>Guidelines for the Operation of CCTV Cameras:</u>

- A Data Protection Impact Assessment must be undertaken for each location to take into account the effect on an individual's privacy and data protection rights, and to

[7] **https://www.lawinsider.com/dictionary/recording-device**

consider if the need identified can be addressed in a less privacy intrusive manner delivering the same objectives. DPIA to be subject to regular review;
- Transparency in its operation of CCTV – Council must let people know they are in an area where CCTV cameras are operational and that CCTV Cameras are recording their personal data. Council should also provide an explanation of why CCTV cameras are in operation, the purpose of the camera and what they are used for. Appropriate signage must be erected to include a published contact point for access to information and complaints;
- CCTV Cameras should not view areas which are not of interest and are not intended to be the subject of surveillance
- In areas where people have a heightened expectation of privacy (for example, toilets, changing rooms etc) cameras should only be used in the most exceptional of circumstances and where they are necessary to deal with serious concerns. In these cases an extra effort should be made to ensure that those under surveillance are aware of the cameras. This may be by way of signs highlighting the fact that there are cameras in operation
- CCTV should not (usually) be used to record audio (for example, conversations between members of the public) as this is highly intrusive
- Regular review and audit of CCTV systems;
- CCTV footage is of sufficient evidential quality (with forensic integrity maintained) and fit-for-purpose.

Use, security and Retention of Recorded Images:

- There should be restricted access to recorded material and recorded images should be viewed in a restricted area or designated office. Access to CCTV recordings should be restricted to authorised personnel only;
- The public should not be allowed access to the area where staff can view CCTV;
- The Council must ensure that images obtained using CCTV are not used for any purpose other than the reason they were originally captured;
- No more footage should be stored than that which is strictly required for the purpose of a CCTV system, and should be deleted once the purpose has been met;
- Access to CCTV footage must be clearly defined, with restrictions on who can gain access and for what purpose;
- Appropriate organisational and technical measures should be in place to protect against unauthorised access and use;
- There should be clear responsibility and accountability within Council for all CCTV in operation;
- Due consideration must be given of approved operational, technical and competency standards and continual work in maintaining such standards;
- Clear rules, policies and procedures (with site-specific operational requirements and protocols) must be in place before a CCTV system is used;
- Regular training must be provided for CCTV operators.

Disclosure of CCTV Images:

- Disclosure of images from CCTV must be controlled and consistent. Requests for images should be treated with care as a wide disclosure may be unfair to the individuals concerned (effectively breaching the DPA/UK GDPR).

- Individuals may request images recorded of them. Such requests should be dealt with formally as Subject Access Requests (SAR) under the DPA/UK GDPR. All such requests should be passed to the Compliance Team as soon as they are received.
- CCTV Images should not generally be released to third parties (although there will be times when this is permissible under the DPA/UK GDPR). Requests for images of third parties should be dealt with formally as requests for information under the Freedom of Information Act. All such requests should be passed to the Compliance Team as soon as they are received.
- Council recognises that individuals have a right to prevent processing of their images where this would cause substantial and unwarranted damage / distress.

RIGHTS OF INDIVIDUALS UNDER THE UK GDPR:

The UK GDPR provides the following rights for individuals:
1.The right to be informed
2.The right of access
3.The right to rectification
4.The right to erasure
5.The right to restrict processing
6.The right to data portability
7.The right to object
8.Rights in relation to automated decision making and profiling.

An individual is entitled to make a request to Council verbally or in writing. For further information visit the ICO's website[8].

BREACHES:

A breach of the DPA/UK GDPR may occur in a variety of ways. For example, this may arise from a theft or accidental loss of personal data (for example, mobile devices, laptops, documents containing personal data). It may also occur due to a deliberate attack on the Council's systems; the unauthorised use of personal data by a staff member or accidental loss or equipment failure. A suspected breach must be reported to the Compliance Team immediately.

Breaches considered 'high risk' need to be reported to the ICO within 72 hours. Failure to notify a breach when required to do so could result in a significant fine, up to 10 million Euros or 2 per cent of turnover.

ICO Penalties:

The ICO has the power to take regulatory action against public bodies for breaches of the DPA/UK GDPR as follows:-

1. The ICO has the power to impose monetary penalties up to the value of 20 million Euros (or equivalent in sterling) or 4% of the total annual turnover in the preceding financial year, whichever is higher;
2. The ICO may issue an Undertaking or Enforcement Notice requiring an organisation to take action or;
3. The ICO has the power to criminally prosecute organisations. Individuals may also be prosecuted under the Act. Upon summary conviction (in a Magistrate's Court) fines

[8] Individual Rights:- https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-UK GDPR/individual-rights/

could result if employees / members process information about other people without their consent or proper authorisation from the Council. Upon conviction or indictment in the Crown Court the fine can be unlimited.

The Council's Breach Management Plan:
Should a breach of the DPA/UK GDPR occur there are four main elements the Council will focus on:

- Containment & Recovery of the breach;
- Assessment of the ongoing risk caused by the breach;
- Notification of the breach and;
- Evaluation of the Council's response to the breach

Council's Breach Management Plan is as follows:

1. All breaches should be notified immediately to the Council's Data Protection Officer/Head of Compliance (or the Assistant Director of Corporate Services (Administration) in their absence) in order that the breach can be addressed. Council hold a Breach Register so that staff can report breaches or potential breaches of DPA/UK GDPR.

2. Upon becoming aware of the breach Council will take all steps necessary to recover the information and limit the damage caused by the breach.

3. Council will assess the risks associated with the breach. In particular it will consider what type of data is involved; how sensitive it is; if data has been lost or stolen; whether there were any protections in place; what has happened to the data; the level of risk posed; how many individuals are affected; who the individuals affected are; what harm can come to those individuals and any perceived wider consequences of the breach.

4. Council will inform the appropriate people and organisations that a breach has occurred. Where appropriate the Information Commissioner's Office and the Police will be informed. The decision to inform the ICO and / or the Police will rest with Council.

5. Council will review its response and take steps to avoid the breach reoccurring.

NOTIFICATION TO THE INFORMATION COMMISSIONER'S OFFICE:
The DPA/UK GDPR requires every Data Controller who is responsible for processing personal data to notify the Information Commissioner's Office that they are processing personal data and to renew their Notification on an annual basis. Failure to do so is a criminal offence.

The Council's Assistant Director of Corporate Services (Administration) is responsible for Council's Notification to the Information Commissioner's Office on an annual basis.

All Officers are required to make the Assistant Director of Corporate (Administration) aware of any changes to the processing of personal data or any proposals to create a new system (paper or automated) which contains personal data. Any changes to Council's Notification should be brought to the attention of the ICO within 28 days.

Time limits

Any person who makes a request to Council for their personal data (subject access request) will be informed without undue delay and at the latest within one month from the date of receipt of their request whether Council holds the information requested. If Council holds the information requested the requester will be provided with the information within one month of the date of receipt the request (subject to legal exemptions). One month is the statutory maximum period within which public bodies must respond to a request. Council will, however, endeavour to provide information to requesters in as short a timeframe as possible. The statutory period of one month may be extended for a further two months in limited circumstances and the requester will be advised if this is the case.

Council may request proof of identity and/or clarification in relation to a request for information. Proof/clarification may be sought in order to assist Council in identifying and locating information relevant to a request. Where Council requires proof/clarification to be provided by a requester Council will inform the requester of this as soon as reasonably possible following receipt of the request. Council will respond to the request when it receives the additional information and within the statutory time limit.

Where Council does not hold the information being requested but Council is aware that another organisation may hold the information Council will advise the requester to contact that organisation and, where possible, will provide contact details for that organisation.

Charging

Under the UK GDPR Council will not charge a fee for most subject access requests. However, Article 12(5) advises where the request is manifestly unfounded or excessive Council may charge a reasonable fee for the administrative costs of complying with the request. This can cover e.g. repeated requests for the same information. In those circumstances, Council will either refuse to respond and explain why, or charge for the administrative costs of providing the information, e.g. photocopying or postage costs; Council cannot, for example, charge for staff time. Council will advise the requester which basis (either manifestly unfounded or excessive) it is relying on.

The ICO's view is that standard requests for personal data will not meet the manifestly unfounded or excessive request threshold, however voluminous the records are.

When an advance payment is required, the requester will be notified and Council will invite the requester to say whether they wish to proceed with the request, or part of it, or whether the request may be met in some other way (for example, by visiting the offices to inspect the information). Where advance payment is required the case will remain active for 60 working days until payment is received. If no payment is received during this time the request closes but the requester may make a new application at any time. When a fee payment is received Council will release the information promptly and within the appropriate time limit.

Exemptions

Schedule 2-4 of the DPA sets out the exemptions to individuals right of access for Council. Officers should consult the Compliance Team for guidance. Some reasons for right of access to be denied is:

- The request is manifestly unfounded or excessive
- Information constitutes the personal data of third parties
- The information is subject to investigation being considered
- Disclosure would prohibit the prevention and detection of crime
- Information is protected under Legal Professional Privilege (LPP)
- Confidential references

Access to information procedure

Introduction

All requests for information (RFI) to Council need to be handled in accordance with the FOIA, EIR and DPA/UK GDPR.

The Information Commissioner's Office (ICO) advises:
"This doesn't mean you have to treat every enquiry formally as a request under the Act. It will often be most sensible and provide better customer service to deal with it as a normal customer enquiry under your usual customer service procedures. The provisions of the Act need to come into force only if:

- *you cannot provide the requested information straight away; or*
- *the requester makes it clear they expect a response under the Act*".[9]

All staff should be familiar with information readily available via Council's publication scheme[10]. The response to such requests should be issued as soon as possible, in adherence with Councils Customer Care procedures and certainly within the statutory time limits.

"*If you need to deal with a request more formally, it is important to identify the relevant legislation:*

- *If the person is asking for their own personal data, you should deal with it as a subject access request under the DPA/UK GDPR.*
- *If the person is asking for 'environmental information', the request is covered by the EIR.*
- *Any other non-routine request for information you hold should be dealt with under the FOIA*".[11]

The Compliance Team (CT) is responsible for processing RFI which fall outside the scope of a "normal day to day business or media enquiry". The CT will acknowledge the RFI, collating the information requested and responding to all requests received by Council. The Head of Compliance/Assistant Director of Corporate Services (Administration) is responsible for responding to internal reviews.

These procedures set out the processes that the CT follow when dealing with a RFI and Head of Compliance/Assistance Director of Corporate Services (Administration) will follow when dealing with a request for Internal Review.

---

[9] In brief - https://ico.org.uk/for-organisations/guide-to-freedom-of-information/receiving-a-request/
[10] Council publication scheme - http://www.newrymournedown.org/publication-scheme
[11] When should we deal with a request as a freedom of information request – https://ico.org.uk/for-organisations/guide-to-freedom-of-information/receiving-a-request/

Types of RFI submitted to Council
There are four different types of request that Council might receive, aside from those which should be dealt with as enquiries in the normal course of business. It is important that the legislation under which a request is made is identified from the outset, as each will be dealt with slightly differently. The CT will identify which piece of legislation the request will be treated under. The requests may be any of the following:

- Requests for information made under FOIA.
- Requests for personal data made under the DPA/UK GDPR.
- Requests for environmental information made under the EIR.
- Request from complainants for information held on their case files which are primarily dealt with under DPA/UK GDPR, with other information on the case file falling outside the DPA/UK GDPR being considered under FOIA or EIR depending on the nature of the complaint (hybrid requests).

All requests under FOIA should be made in writing. Verbal requests are valid under EIR and DPA/UK GDPR. Verbal requests can be captured using the ICO's verbal request template form[12].

Council has a duty to comply with Section 49A of the Disability Discrimination Act 1995 (as amended by the Disability Discrimination (NI) Order 2006. The CT will support individuals requiring assistance in submitting requests in accordance with Chapter 6 of Councils Equality Scheme[13].

Receiving and acknowledging a RFI
The CT receives requests:

- Directly from individuals via telephone, letter or email addressed to the CT; and/or
- Communications which are transferred by teams to CT, including through social media.

All RFI to be dealt with by the CT will be logged on the monitoring spreadsheet as cases and given a reference number. New requests should be given a new case reference number from the central filing database. Existing case reference numbers can be applied to routine follow up requests that can be processed quickly.

The request case will be set up and an acknowledgement sent to the requester within two working days. The acknowledgement will clearly state the date by which the requester can expect a response. *If a response can be issued within two working days, an acknowledgement will be included therein.

Establishing whether the request is valid

[12] Saved on the R Drive, under 'Policies and Procedures' folder
[13] Council's Equality Scheme - http://www.newrymournedown.org/equality

The first stage once a request has been received is establishing whether it is a valid request:

- is it in writing (required for FOIs) or verbal (accepted under DPA/UK GDPR & EIR)
- does it contain the name and an address for correspondence?
- Is a form of ID required (DPA/UK GDPR)?
- does it describe the information being requested?

Seeking clarification
At the stage of acknowledgement, the CT will assist and advise requesters on what information is required to process their request.

Examples of the most common instances where the CT seeks clarification include; asking for proof of ID or authorisation (when dealing with a SAR on behalf of another individual. Where the request is not clear, can be read in more than one way or the CT has not received enough information needed to locate and retrieve the information being requested, clarification will be sought from the requester rather than attempt to interpret the scope of the request.

The case is closed in the acknowledging team member's name pending the receipt of the requested clarification. Once the clarification is received, the case is then reopened, acknowledged and referred back for processing.

Requests which can be responded to immediately
The request may be for information which, although not included in the Publication Scheme, can be provided immediately, or is for information which is not held by Council.

In either of these circumstances the response will be sent immediately, and the case closed. Where the information is not held Council will explain why and, if the request is misguided, provide the contact details for the correct organisation if known.

Advice may be sought by members of staff outside the CT regarding requests that can be responded to as normal course of business. Such requests should be responded to promptly, in adherence with Councils Customer Service Standards and certainly within the statutory timeframe.

Gathering and collating the information
Having interpreted the request, the CT will conduct searches of electronic and manual records, accessible to the CT, to establish what information is held. The monitoring spreadsheet and previous responses will also be considered when gathering information, noting any lapsed time.

The CT will then identify the possible Department(s) which may hold any additional information. The Department is added on the monitoring spreadsheet and an e-mail sent to the Head of Service (or equivalent) and responsible officer as soon as possible to allow them a reasonable time to respond.

When consulting with teams, the CT will:

- Clearly specify the information requested

- Enquire whether information which falls within the scope of the request is held by the department

- Specify a date by which a response should be provided to the CT (usually at least one week before the request is due)

- Ask for any views that the Department may have on disclosing the information

- Ask for any additional information which might put the information being requested into context and provide additional assistance to the requester.

In some cases, it may be necessary to send an 'all staff' email to ask staff to check their computers and manual files for information covered by the scope of the request. The requesters personal information will not be disclosed to third parties, unless a lawful basis applies.

Classification of Information
Information that contains protective marking e.g. 'Personal', 'Confidential' and/or 'Sensitive' will be considered in line with any applicable exemptions and or guidance from the ICO.

Cost
Council will adopt a 'in favour of disclosure approach'. In exceptional circumstances Council may consider refusing to comply with a request on the basis of the costs involved. If the information is held, the CT will estimate whether the cost of complying is "reasonable".

- Under FOI the cost limit is £25 per hour, £450 or 18 hours.

- Under EIR there is no cost limit. Manifestly unreasonable requests will be subject to a public interest test and, if applicable, a reasonable fee.

- Under DPA/UK GDPR there is no cost limit. Manifestly unfounded or excessive requests will be subject to a reasonable fee.

Where the CT receives multiple requests, but each individual request is for information falling under only one access regime (FOIA, EIR, or DPA/UK GDPR) then there will be no aggregation of costs across the different access regimes. In this situation the CT will only take the aggregated costs of responding to FOI requests into account under FOIA. Similarly, the CT will only take the costs of responding to requests for environmental information into account when deciding if multiple similar requests are manifestly unreasonable/unfounded under the EIR and DPA/UK GDPR[14].
If a request exceeds the reasonable/appropriate cost limit the table below identifies the description of costs which can be applied under the relevant regime:

[14] ICO - Calculating a cost where a request spans different access regimes: https://ico.org.uk/media/for-organisations/documents/1192/calculating_costs_foia_eir_guidance.pdf

Cost description	FOI[15]	EIR[16]	DPA/UK GDPR[17]
Time	Only chargeable if the info cannot be viewed by the requester at a Council site		X
Printing / copying The Council will not charge for photocopying which amounts to less than £5.00	✓	✓	No cost for one copy. Cost applied for additional copies.
Postage	✓	✓	✓
Format (*media device, Folder/ring binder*)	✓	✓	✓

The requester will be advised of the fees notice and advice to enable them to reformulate their request to try bring it within the cost limit which will be treated as a new request. They will also be advised of the date to pay the fees notice (60 working days) or respond with a reformulated request.

The CT will also advise requesters they can seek an Internal Review of fees notices.

Consultation
If the information requested includes correspondence or information provided by a third party it may be necessary for the CT to contact that individual or organisation to seek their views on the disclosure.

The communication with the consultee will specify the document(s) considered for disclosure, and where necessary the CT may also need to provide a copy of the information considered for disclosure. A time frame for the reply will be given to the third party consulted.

The requesters personal information will not be disclosed to third parties, unless a lawful basis applies.

Responding to a request
The CT will adhere to the following checklist:

- Log all SAR/FOI/EIR requests on the monitoring spreadsheet.
- Review the monitoring spreadsheet to ascertain repeat requests and responses.

[15] ICO – Fees that may be charged when the cost of compliance exceeds the appropriate limit: https://ico.org.uk/media/1635/fees_cost_of_compliance_exceeds_appropriate_limit.pdf
[16] ICO – Charging for Environmental Information: https://ico.org.uk/for-organisations/foi-eir-and-access-to-information/freedom-of-information-and-environmental-information-regulations/charging-for-information-under-the-eir/#:~:text=Regulation%208%20of%20the%20EIR,ability%20to%20exercise%20that%20right
[17] ICO – Can we charge a fee: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-UK GDPR/individual-rights/right-of-access/

- Consider ICO guidance and decision notices.

- New requests should be given a new case reference number from the central filing database. Existing case reference numbers can be applied to routine follow up requests that can be processed quickly.

- Is the request from an individual for information about their case/complaint? If so, generally in the first instance treat it as a DPA/UK GDPR subject access request but bear in mind that some information in the file may need to be considered for disclosure under FOIA or EIR.

- If treating as a subject access request and records held are historical (e.g. an application prior to 25 May 2018) then the request should be considered under the DPA/UK GDPR 2018. The DPA 1998 is only relevant if reviewing a decision and the matter is still ongoing.

- Is the information already available through Council's Publication Scheme or are they able to book an appointment to view files?

- Where necessary offer advice and assistance as soon as possible.

- Issue acknowledgement* within two working days (see * on page 21).

- Advice and assistance should be offered if the request is vague or framed as a question:

    - Give as much information as possible in normal course of business
    - Check whether they still require further information
    - Explain the right to request recorded information
    - Explain what sort of information we might hold

- In every case where advice and assistance is provided:

    - Check we have understood what information they require
    - Explain what happens next in considering their request
    - Confirm date of receipt and latest date for response

- Search for the information. If the search would exceed the cost limit contact the requester as soon as possible, issue fees notice, date for payment and offer to assist reformulating the request.

- If Council does not hold any information, contact the requester to explain this. Offer advice on who else may hold the relevant information.

- If Council holds the information, is there a good reason not to disclose it? For example, does an exemption/exception apply

- Are there any protective markings e.g. draft, sensitive, private, confidential?

- Are there any FOI/EIR/DPA/UK GDPR disclosure notices contained within documents?

- Has the requester specified a preferred means of communication?

- Does Council need to consult with a third party (e.g. employee, contractor, stakeholder) before deciding on whether to disclose or withhold the information under an exemption?

- If Council wants to withhold the information, can it provide redacted documents?

- Is the request voluminous or sensitive and require peer checking?

- If Council withholds or redacts any information, issue a Refusal Notice. Include:

    - A confirmation that Council holds the information (unless an exemption applies to the confirmation itself)
    - The section and subsection of the exemption
    - Why the information falls within the exemption (unless explanation would disclose exempt information)
    - If prejudice-based, an explanation of likely prejudice
    - If qualified, set out the public interest arguments for and against disclosure
    - If absolute, explain there is no public interest test requirement
    - How to request an internal review and how to appeal

- Has the requesters address been checked against the original request?

Responses to requests will be sent as soon as the information is available. In some cases it may be possible to respond immediately, upon receipt, in which case it is not necessary to send an acknowledgment.

The information contained within the response will vary according to the nature of the request. Generally, a response to an FOI/EIR request should initially confirm whether or not the information requested is held, although there is some variation to this.

In cases where information is withheld, a Refusal Notice will be issued. The CT will set out the exemption(s) applied, the public interest (if applicable) and the reason why the exemption is engaged.

The CT will keep a copy of all documentation on file in response to the request. The CT will label the copy of un-redacted information in case it is subject for future request, Internal Review or review by the ICO.

The CT will:

- ensure to have complied with any reasonable request for a particular format, electronic or hardcopy
- ensure that the correct review or right of appeal paragraphs are included
- check any attachments or enclosures which are being provided in response to the request before sending out the response

- ensure attachments to email are sent via pdf and encrypted/password protected where appropriate
- check the postal or email address of the requester against the original request before sending out the response. Place sensitive/confidential information within a second envelope for extra protection.
- Update the monitoring spreadsheet

Internal Reviews
The CT will acknowledge receipt of the request for review as soon as it is received and give the latest date by which the requester can expect a response.

The Head of Compliance/Assistant Director of Corporate Services (Administration) will conduct Internal Reviews and request the relevant file from the CT, to include:

- The original request
- The response
- Copies of information (guidance, verbal discussions etc)
- Copies of consultation request & responses
- Copies of unredacted information where applicable
- Request for review
- Acknowledgement

The Head of Compliance/Assistant Director of Corporate Services (Administration) will review the original decision, taking account of any time lapse and ICO decision notices. The response will include the details of the review, the outcome and requesters right to complain to the Commissioner. The respective file will be updated to include records of the Internal Review and the monitoring spreadsheet.

Roles and Responsibilities

Responsibilities of Council Officers
All Council Officers who hold or process recorded information held by Council are responsible for complying with the FOI/EIR/DPA/UK GDPR legislation and this procedure.

RFI can be made to any Council Officer. All Officers who receive RFI that cannot be dealt with within the normal everyday requirements of their role and function should forward the request to the CT immediately. If an Officer is in doubt as to whether a RFI requires to be dealt with under the terms of the FOI/EIR/DPA/UK GDPR the Officer should immediately contact the CT. All transfers of requests to the CT should be made immediately upon receipt of the request to allow the CT sufficient time to deal with the request within the statutory timeframe. Where an Officer deals with a RFI within the normal everyday requirements of their role they should be aware of the statutory timeframes.

When requested by the CT to provide information requested under the FOI/EIR/DPA/UK GDPR all Council Officers must provide all information held by them in relation to the request. Officers can highlight any sensitives over the disclosure of information, but it is the CT who decides whether an exemption/exception is engaged. If an Officer is unsure whether information they hold is relevant to a request they should check this with the CT.

Information held in non-work personal email accounts may be subject to the legislation if it relates to the official business of Council. When a request for information is received Officers should consider all locations where relevant information is held, including private email accounts.

Council acknowledges that personal data held on private email accounts relating to the official work of the Council, falls within the scope of a request for information. However, since private email accounts may not be subject to the level of security deemed appropriate by the Council, storing personal data and using private email accounts risks breaching Article 5 and Article 32 of the UK GDPR.

Private email accounts should only be used in **exceptional** circumstance, for example, if Councils official IT platform is down and the matter requires urgent action. When communicating to a data subject regarding Council official business using a private email account, you must cc your official Council email address to ensure completeness of Council records[18]. Officers communicating via their private email account or are otherwise transmitting and/ or storing data therein, engage the data protection principles. **Officers therefore should use their Council email address and secure Council devices when communicating to data subjects regarding Council business.**

Whilst the Council has a statutory maximum statutory timeframe within which to respond to a request Officers will be required to provide the CT with the requested information within the timeframe as specified by the CT. This to ensure that the CT has sufficient time within which to consider the information, contact relevant third parties and redact exempt information where necessary.

It is a criminal offence to wilfully conceal, damage or destroy information in order to avoid responding to a request. It is therefore important that no records that are the subject of a request are amended or destroyed. The ICO advises: "*where information that is covered by a request is knowingly treated as not held because it is held in a private email account, this may count as concealment intended to prevent the disclosure of information, with the person concealing the information being liable to prosecution*".[19]

All Council Officers are also responsible for good information handling practice and implementing records management policies and procedures as appropriate. Council departments are responsible for the content of the Publication Scheme and must review it regularly. Departmental website content updates should be forwarded to the Marketing and Communications Team and Compliance Team for inclusion on the website.

When a request is made for information and that information includes the names of employees in connection with their work on behalf of Council, as a general rule Heads of Service and above name, job title and/or role will be disclosed.

The question of disclosure of employee's name, job title and/or role below Head of Service will be looked at on a case by case basis. The main consideration in deciding whether to

[18] Official information held in private email accounts, p5:- https://ico.org.uk/media/for-organisations/documents/1147/official_information_held_in_private_email_accounts.pdf
[19] Page 4, link as above.

release the information in connection with their work on behalf of Council will be whether it is fair in all the circumstances to identify an individual employee e.g. whether they have been involved in the decision making process and whether their information is already in the public domain. Special consideration will be given where the disclosure of an employee's name would cause unwarranted damage or distress to that individual.

Responsibilities of Councillors

Information received, created or held by a Councillor on behalf of the Council will be covered by the legislation. This includes information received, created or held by a Councillor outside of the Council Chamber / Council Offices where the information forms part of their work as a Councillor on behalf of Council. Correspondence between Councillors or information held by a Councillor for their own private, political or representative purposes will not usually be covered.

As Councillors are not public authorities in their own right they have no obligation to respond to a request for information addressed to them individually. However, as a matter of good practice, a Councillor should explain this to the requester and, with the permission of the requester, pass the request to the CT. All transfers of requests to the CT should be made immediately upon receipt of the request to allow the Officer sufficient time to deal with the request within the statutory timeframe.

When requested by the CT to provide information requested under the FOI/EIR/DAP/UK GDPR all Councillors must provide all relevant information held by them in their role as an agent or representative on behalf of Council. Councillors can highlight any sensitives over the disclosure of information, but it is the CT who decides whether an exemption/exception is engaged. If a Councillor is unsure whether information they hold is relevant to a request they should check this with the CT.

Information held in non-work personal email accounts may be subject to the legislation if it relates to the official business of Council. When a request for information is received Councillors should consider all locations where relevant information is held, including private email accounts.

Council acknowledges that personal data held on private email accounts relating to the official work of the Council, falls within the scope of a request for information. However, since private email accounts may not be subject to the level of security deemed appropriate by the Council, storing personal data and using private email accounts risks breaching Article 5 and Article 32 of the UK GDPR.

Private email accounts should only be used in **exceptional** circumstance, for example, if Councils official IT platform is down and the matter requires urgent action. When communicating to a data subject regarding Council official business using a private email account, you must cc your official Council email address to ensure completeness of Council records[20]. Councillors communicating via their private email account or are otherwise transmitting and/ or storing data therein, engage the data protection principles. **Councillors therefore should use their Council email address and secure Council devices when communicating to data subjects regarding Council business.**

[20] Page 5, link as above.

Whilst the Council has a statutory maximum statutory timeframe within which to respond to a request Officers will be required to provide the CT with the requested information within the timeframe as specified by the CT. This to ensure that the CT has sufficient time within which to consider the information, contact relevant third parties and redact exempt information where necessary.

It is a criminal offence to wilfully conceal, damage or destroy information in order to avoid responding to a request. It is therefore important that no records that are the subject of a request are amended or destroyed. The ICO advises: "*where information that is covered by a request is knowingly treated as not held because it is held in a private email account, this may count as concealment intended to prevent the disclosure of information, with the person concealing the information being liable to prosecution*".[21]

Councillors should be aware that where their names appear on any recorded information or documentation held by them or by the Council in connection with their work on behalf of the Council their names and position within the Council will ordinarily be disclosed as a matter of course.

Training

All staff and Councillor's will be provided with mandatory FOI/EIR/DPA/UK GDPR training which will be required to be undertaken every three years, subject to legislative amendments. Refresher guidance will be provided annually.

FOI/EIR/DPA/UK GDPR training will form part of the Council's induction for new employees. A copy of this policy and procedure will be provided to all employees and Councillors.

Monitoring and Review

To ensure this Procedure complies with the terms of the FOI/EIR/DPA/UK GDPR and meets the needs of Council it will be reviewed every four years. If there is a change in legislation and/or internal processes review may complete sooner.

[21] Page 4, link as above.