Comhairle Contae
Fhine Gall
Fingal County
Council

DATA PROTECTION POLICY

Contents

1. Introduction

Fingal County Council ('the Council") is the democratically elected unit of Local Government in the administrative County of Fingal and is responsible for the provision of an extensive and diverse range of services to the people of the County.

In order to provide the most effective and targeted range of services to meet the needs of the citizens, communities and businesses in Fingal, the Council is required to collect, process and use certain types of information about people and organisations. Depending on the service being sought or provided, the information sought may include 'personal data' as defined by the Data Protection Act 2018 and by the General Data Protection Regulation (GDPR) and may relate to current, past and future service users; past; current and prospective employees; suppliers; and members of the public who may engage in communications with our staff. In addition, staff may be required, from time to time, to collect, process and use certain types of personal data to comply with regulatory or legislative requirements.

2. Definitions

GDPR: General Data Protection Regulation

Consent: Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Data Breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or, or access to, personal data transmitted, stored or otherwise processed.

Data Controller: A person who, either alone or with others, controls the contents and use of personal data.

Data Processor: An entity that processes personal data under the Data Controller's instructions.

Data Subject: An individual who is the subject of personal data. For example, staff members, clients and vendors.

Lawful basis for processing personal data: In order to process personal data an organisation must have a lawful basis to do so.

Personal Data: Any information relating to an identified or identifiable natural person; 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.

Data Protection Impact Assessment (DPIA): A process designed to identify and address the privacy issues of a particular project. It considers the future consequences of a current or proposed action by identifying any potential privacy risks and then examining ways to mitigate or avoid those risks.

Processing: Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated mean, 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.

Recipient: A natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

Special Categories of Data: Special categories of data is defined in the Data Protection Acts as any personal data as to -

> (a) the racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject

(b) whether the data subject is a member of a trade union

(c) the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person,

(d) the physical or mental health or condition or sexual life of the data subject

(e) the commission or alleged commission of any offence by the data subject, or

(f) any proceedings for an offence committed or alleged to have been committed by the Data Subject, the disposal of such proceedings or the sentence of any court in such proceedings.

3. Responsibilities of Staff and Data Protection Officer

Staff:

1. Be aware of the Council's data protection requirements, and their roles and responsibilities in relation to their implementation.
2. Maintain personal data as confidential and secure at all times.
3. Be bound by a duty of confidentiality

Data Protection Officer

Under Article 37 (1) the controller and the processor shall designate a data protection officer in any case where: (a) the processing is carried out by a public authority or body.

On 31st July 2018 Fingal County Council appointed a Data Protection Officer by Chief Executive Order.

In addition to supporting an organisation's compliance with the Data Protection legislation, DPOs will have an essential role in acting as intermediaries between relevant stakeholders e.g. supervisory authorities, data subjects and business units within an organisation.

4. Principles of GDPR

Principle 1 Obtain and Process data fairly, lawfully and transparently

The GDPR requires that the council must have a valid lawful basis for collecting and processing any of the personal data being processed.

Under GDPR there are six lawful bases for the processing of personal data which can be relied upon:

(a) Consent: The basis of consent requires a very clear and specific statement of consent for their personal data to be processed for specific purpose with a positive opt-in .

(b) Contract: the council can rely on this lawful basis if they need to process personal data to fulfil contractual obligations or because they have requested specific steps are taken before entering into a contract (e.g. contract of employment, contract to provide booking engine). The processing must be necessary to fulfil these obligations.

(c) Legal obligation: the council can rely on this lawful basis when the processing is necessary to comply with a statutory obligation (not including contractual obligations)

(d) Vital interests: the council can rely on this lawful basis where the data processing is required to protect someone's life.

(e) Public task: An organisation can rely on this lawful basis 'in the exercise of official authority' or to perform a specific task in the public interest that is set out in law.

(f) Legitimate interests: the processing is necessary for the legitimate interests of the council 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. As a public authority this will not apply to the council when carrying out its duties as set out in legislation but there are limited circumstances where it may be applicable.

The council must determine the lawful basis, or reason, for collecting and processing personal data before initiating a process. The following should be considered:

1. The lawful basis for the collection and processing of personal data must be provided to the Data Subject in advance of the data collection.
2. Where consent is used as the lawful basis, it must be freely given, specific, informed and unambiguous. When relying on consent, the council shall:
    - Provide clear information on what the consent relates to;
    - Give the Data Subject sufficient information to make a choice;
    - Explain the different ways the council shall use their information;
    - Provide a clear and simple way for the Data Subject to indicate they agree to different types of processing. The consent forms shall provide Data Subjects with the choice to consent to their information being used for one purpose but not another.
3. Consent may be withdrawn at any stage and separate consent must be obtained for different processing operations
4. The council shall have information materials and guidance that explains how the personal data of Data Subjects, including staff, is used. This shall be provided in a format that can be easily understood, such as a Privacy Notice/Statement. The Council's Privacy Notices can be viewed at https://www.fingal.ie/council/service/data-protection.

In respect to transparent processing, Fingal County Council has in place a number of privacy statements which advise customers and citizens of their privacy rights when providing personal data to the council for processing for different purposes s well as other policies, such as for CCTV, which are available on the Council website at https://www.fingal.ie/council/service/data-protection. All policies and privacy notices are subject to constant review.

Principle 2 Keep personal data only for one or more specified, explicit and lawful purposes

1. The council must inform Data Subjects of the purpose of collecting and storing personal data. The purposes of the processing must be precisely and fully identified prior to, or at the moment of the collection.
2. Personal Data can only be used for the purpose the council has specified it was collected for.
3. Personal data collected for a specific purpose may be further processed for different purposes provided that these are not incompatible with the initial purposes. If the council wishes to change or add an additional purpose which is not compatible with the original purpose, then the Data Subject must be made aware of the additional purpose for which the personal data will be processed.
4. Individuals have the right to request that the council restricts the processing of their personal data in the following circumstances:
    - the individual contests the accuracy of their personal data and the council is verifying the accuracy of the data;
    - the data has been unlawfully processed (i.e. in breach of the lawfulness requirement of the first principle of the GDPR) and the individual opposes erasure and requests restriction instead;
    - The council no longer needs the personal data but the individual needs the council to keep it in order to establish, exercise or defend a legal claim; or

- An individual can make a request for restriction verbally or in writing and the council has one calendar month to respond to a request.

Principle 3: Personal data shall be used and disclosed only in ways compatible with these purposes

As in Principle 2 above, the council must inform Data Subjects precisely of the purpose of collecting and storing the personal data prior to, or at the moment of the collection.

Principle 4: Keep it safe and secure

Any changes to the council processes, that may impact on the quality and safety of the service provided, shall be managed in accordance with Change Management. As part of this process, proposed changes shall be considered in relation to the potential impact on the safety and security of personal data. Where appropriate, through the use of Data Protection Impact Assessments (DPIA's), the council shall embed data privacy features and data privacy enhancing technologies directly into the design of projects at an early stage. This shall ensure that all required controls are implemented to protect Data Subjects' personal information prior to the implementation of the change and therefore implementing data protection by design.

Principle 5: Keep it accurate, complete and up-to-date

The council has an obligation to ensure that only accurate personal data is held on file. Personal data should be kept up-to-date at all times and corrected where necessary.

Principle 6: Ensure that it is adequate, relevant and not excessive

1. The council must make sure personal data is adequate and is processed/used fairly and effectively. The information sought should be:
    - Adequate in relation to the purpose(s) for which it was sought.
    - Relevant in relation to the purposes for which it was sought.
    - Not excessive in relation to the purposes for which it was sought.
2. Data Controllers must not ask for, process, or hold, personal data that is not relevant or needed for the purpose(s) for which it was obtained.
3. Data deletion and destruction controls are implemented as detailed in the Data and Records Management Policy, and in the relevant National Retention Policies for Local Authority Records (see https://www.fingal.ie/council/service/data-protection for copies of retention schedules by Council service/function)

Principle 7: Retain it for no longer than is necessary for the purpose or purposes

1. The Council ensures there is a clear policy for the retention and disposal of personal data no longer required. The retention times for personal data will vary from purpose to purpose. The Council follows the relevant LGMA National Retention Policies for Local Authority Records as they are issued and revised (see https://www.fingal.ie/council/service/data-protection for copies of retention schedules by Council service/function)

Principle 8: Give a copy of his/her personal data to an individual, on request

The council must comply with a Subject Access Request under GDPR within 1 month.

5. Personal Data Protection and Security Measures

The council implements a collection of effective data security measures for personal data. In deciding what level of security is appropriate, the council shall have regard to the nature of the personal data in question, and the harm that might result from unauthorised use, disclosure or loss of the personal data.

Physical Securities for Hardcopy Personal Data

1. The designated location utilised to retain personal data records shall have secure windows, doors and a controlled access system. This location shall allow for controlled access and speedy retrieval of records when and where they are required by authorised individuals but also provide controls to prevent unauthorised access.
2. Personnel data shall be protected from hazards such as fire, flooding, temperature, humidity, atmospheric pollution and vandalism by use of a fire proof cabinet that can be locked when not in use. The keys of locked filing cabinets shall be stored in a secure location and staff are prohibited from taking such keys home.
3. All staff shall ensure that personal data is guarded securely at all times and shall take care to ensure that the Data Subjects information is not placed in any public place or where it may be viewed or accessed inappropriately.
    a. Personal data shall not be left on desks in offices in the absence of the responsible staff. Whenever an office is left unattended it should be securely locked.
    b. All personal data records shall be returned to their appropriate storage facility as soon as reasonably possible after use.
4. All waste papers, printouts, etc. of personal data shall be stored in secure lockable confidential waste bins that have a bin top or slot through which confidential waste can be placed but not retrieved. This applies to all areas of the council, including office areas to which access is restricted to staff. Waste paper shall be disposed of via confidential shredding by an approved supplier.
5. Where key pad access controls are in use for certain areas of the council, the key codes shall be changed periodically.
6. Keys of locked offices should be stored in a secure location and staff shall be prohibited from taking such keys home at the end of their shift.
7. Postal correspondence, such as incoming and outgoing letters, that is awaiting collection or further distribution within the council, shall be held in a secure environment.

Software Securities for Data

Where the records of Data Subjects are retained via software systems, the council shall use technical security measures to protect the data. Minimum standards of security implemented by the council shall include the following:

1. Implementation of software controls to prevent external hacking and access by the cloud provider's personnel or by other users. Anti-virus software shall be used and shall be kept up to date.
2. Access to central IT servers shall be restricted in a secure location with only a limited number of staff having access. The access for these individuals to the central IT server are approved by the council, including any non-authorised staff or contractors.
3. Secure backup systems shall be in place for vital personal data. There shall be a back-up procedure in operation for data held on computers. This shall include an off-site back up.
4. Data on computer screens should always be hidden from the view of passers-by . Computer screens shall be set to automatically lock and log users off after a certain short period of inactivity. A screen saver shall appear on locked screens to ensure that no personal data remains visible.
5. Individual passwords for systems shall be used to stop unauthorised access to records. PC's and laptops shall utilise encryption software. The standard of encryption shall be sufficiently robust to withstand attacks from newly-developed decryption software.
6. Transmission of personal data over external networks, such as the internet, should normally be subject to robust encryption.
7. Access to personal data held in soft copy will be allocated in accordance to the roles and responsibilities of the staff member.

8. Staff are prohibited from accessing or editing, via other users' accounts, the records of personal data on the council's computer systems
9. Where IT management and securities are managed by an external supplier, the supplier shall be formally approved, and a Data Processing Agreement shall be in place covering the security of the data that meets or exceeds the assessed level of protection required.
10. The Data Subject's personal information shall not be discussed by staff outside the council or in the council corridors, lifts or canteen.

6. Data Processing Agreement

All data processing arrangements with third party service providers shall meet the requirements of the Data Protection Acts 1988 to 2018 and the requirements of the GDPR.

Where the council engages the services of a Data Processor, it shall take certain steps to ensure that the data protection standards are maintained. A Data Processor shall be engaged to complete data processing for the council under a written contract, which details appropriate data securities and safeguards.

Any contract utilised for the engagement of a Data Processor shall specify:

- The subject matter of the data and duration of the processing.
- The type of personal data and categories of data subject.
- The obligations and rights of the council as the Data Controller.
- The instructions as to what the Data Processor can do with the personal data provided.
- The nature and purpose of the processing, that the Data Processor will process personal data only on the basis of the authorisation and instructions received from the Data Controller. This provision ensures that personal data passed on to a Data Processor may not be retained or used by the data processor for its own purposes.
- That the Data Processor must be committed to apply appropriate security measures to the personal data to protect it from unauthorised access or disclosure. This provision ensures that the standard of security must be maintained when the personal data is passed from the council to its agent.
- That the Data Processors ensure that people processing the personal data are subject to a duty of confidence.
- That the Data Processors may only engage sub-processors with the prior consent of the council and under a written contract.
- That the Data Processors assist the Data Protection Officer in providing Subject Access Requests and allowing Data Subjects to exercise their rights under the GDPR.
- Any penalties in place should the terms of the contract be broken by the Data Processor.
- That the council or their agents have a right to inspect the premises of the Data Processor as to ensure compliance with the provisions of the contract.
- That the Data Processor must submit to audits and inspections by the council to ensure compliance with the provisions of the contract, or by the Office of the Data Protection Commission, and provide the council with whatever information it needs to ensure that they are both meeting their Article 28 obligations.
- That the Data Processor shall tell the council immediately if there is a personal data breach or is asked to do something infringing the GDPR or other data protection law of the EU or a member state.
- That the Data Processor must register with the Office of the Data Protection Commission for the duration of the contract.
- That the deletion or return of the data is required upon termination or ending of the contract.

7. Retention and Disposal of Personal Data

Fingal County Council implement its Data and Records Management Policy throughout the organisation. This is done via its new EDRMS system, called FinDocs.

The policy and records management system are designed to ensure that there is a standardised electronic/digital filing system in which data is securely held and is readily accessible and retrievable in the event of a Subject Access Request and/or a Freedom of Information request.

In order to ensure a standardised e-filing methodology, guidance and training on the use of electronic drives, including naming and usage of E-Cabinet and E-folders and subfolders, and the categorising and filing of emails has been and will continue to be issued to staff.

Data and information may be held in the following formats:

- Paper records, application forms etc.,
- Text Messages
- Electronic Files on FinDocs, shared and standalone drives,
- Emails,
- Diaries,
- Accounts,
- Registers,
- Note Books,
- Servers,
- Website., Intranet.
- Drawings, Maps etc.
- Photographs/images/videos
- Micrographic materials (e.g. microfilm, microfiche)
- CCTV/drone footage

Further guidelines for retention and disposal of personal data:

1. Information should not be retained once the initial purpose has ceased, unless there is a clear lawful basis. The council recognises that personal data cannot be retained just in case the Data Subject makes a request at some time in the future. The council shall not retain personal data for any purpose for longer than is necessary.
2. The retention records created by the council is specified under relevant regulation such as the National Records Retention Policies for Local Authority Records (see https://www.fingal.ie/council/service/data-protection for copies of retention schedules by Council service/function)
3. After the retention period has passed, the records shall be destroyed under confidential conditions, e.g. secure shredding, comprehensive electronic deletion with certification of deletion/destruction, and in line with environmental health regulations.
4. Under the Data Protection legislation, a Data Subject has the right to request all information held in relation to them be destroyed, however this right is not absolute, e.g. a staff member who has had their employment terminated may request their personal data is destroyed, however if there is a lawful reason why this personal data must be retained such as a legal claim, the council can refuse and continue to retain it in accordance with the council's determined retention periods. This shall be dealt with on a case by case basis by the Data Protection Officer.
5. In certain situations, the Data Subject may have the right to request personal data be moved. This request shall be supported by the Data Protection Officer.

8. Personal Data Breach

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

Where staff identify that a possible personal data breach has occurred, they shall report this to the Data Protection Officer via the email Data.Officer@fingal.ie.

The Data Protection Officer shall complete an investigation to quickly establish whether a personal data breach has occurred. Where required, additional support shall be sourced to investigate the possible breach, e.g. IT Support Services, external Data Processers, etc.

Where it is found that a personal data breach has occurred, the Data Protection Officer shall establish the likelihood and severity of the resulting risk to the Data Subject's rights and freedoms.

Data Controllers do not have to notify the Office of the Data Protection Commission if the breach is unlikely to result in a risk to the rights and freedoms of Data Subjects. Even where there is no obligation to notify the breach, the council must still document the breach and the steps taken to resolve it and to prevent it from occurring again.

If it's likely that there is a risk to personal data then the Office of the Data Protection Commission must be notified without undue delay, but not later than 72 hours after becoming aware of it. In case of doubt, in particular any doubt related to the adequacy of technological risk-mitigation measures, the council should report the incident to the Office of the Data Protection Commission.

When reporting a breach to the Data Protection Commission, the following must be provided:

- a description of the nature of the personal data breach including, where possible:
- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- the name and contact details of the Data Protection Officer, or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

The Data Subject(s) shall be notified of the personal data breach promptly by the council if there is a high risk that their personal data has been obtained or used inappropriately. Supports shall be provided by the council to the affected parties. The information to be provided to the Data Subjects in clear and plain language include:

- the nature of the personal data breach;
- the name and contact details of the Data Protection Officer;
- a description of the likely consequences of the personal data breach;

- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

The Data Protection Officer shall make themselves available to the Data Subject to discuss the issue further and shall provide the Data Subject with ongoing updates relating to the investigation and close out.

In appropriate cases, the Council should also notify organisations that may be in a position to assist in protecting data subjects including, where relevant, An Garda Síochána, financial institutions etc.

All appropriate actions shall be taken by the Council, in conjunction with the Data Protection Officer, to contain the breach, assess and address the potential adverse consequences for individuals and address the root cause of the breach to prevent reoccurrence. The Council recognises that Data Controllers can be subject to large fines, unless they can demonstrate appropriate measures were taken to ensure the personal data was safe and secure.

Following containment of the breach, the Data Protection Officer, in conjunction with the Council, shall review the incident to consider what lessons can be learnt from the breach and the Council's response to the breach.

All personal data breaches, whether reportable to the Office of the Data Protection Commission or not, shall be documented within the data breach process. The Breach Report Form shall document the facts relating to the breach, its effects, the roles and responsibilities and the remedial actions taken to contain an incident and rectify it as appropriate. These records should be provided to the Office of the Data Protection Commission upon request.

Where the council utilises a Data Processor, and this processor suffers a breach then the Data Processer is required to inform the Council's DPO without undue delay as soon as it becomes aware of the breach. As the Data Controller, the council is then required to notify the Data Protection Commission.

9. Right of Access – Subject Access Requests

Under the Data Protection Acts 1988 to 2018 Data Subjects have a right to obtain a copy, clearly explained, of any information relating to them that is kept on computer or in a structured manual filing system or intended for such a system by any entity or organisation.

The council recognises that Data Subjects are entitled to:

- a copy of the data the council is keeping about him or her;
- know the categories of their data and the council's purpose/s for processing it;
- know the identity of those to whom the council discloses the data;
- know the source of the data, unless it is contrary to public interest;
- know the logic involved in automated decisions;
- data held in the form of opinions, except where such opinions were given in confidence and even in such cases where the person's fundamental rights suggest that they should access the data in question it should be given.

All Subject Access Requests must be made to the Data Protection Officer. This will normally be made in writing. Fingal County Council provides a Data Subject Access Form at on the Council website https://www.fingal.ie/sites/default/files/2020-11/fingal-county-council-sar-subject-access-request-form-nov-2020.pdf to ensure all required information is provided to quick respond to the request.

On receipt of the request from a Data Subject, where appropriate, the Council shall verify the identity of the person making the request, using 'reasonable means. If a request is received and the Council is not

satisfied as to the person's identity, evidence of identity may be required from the requestor. This shall be applied where it is deemed necessary and where there is a risk of disclosing personal data to a third party.

Where a DSAR is received which involves the release of CCTV footage, this can be released in two forms:

- A video copy of the footage
- Still images (photograph) taken from the camera. Where still images are provided, they shall be at a rate of one photograph per second of video.

However, Data Controllers can only provide copies of a person's own personal data. This cannot include the personal data of another party.

If the request is made electronically, the personal data shall be provided in a commonly used electronic format. Where the information is being sent by post it shall be sent by registered post, double wrapped and marked confidential. However, personal information shall never be provided to individuals over the phone.

Copies of the personal data information must be provided free of charge; however, the council can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.

A reasonable fee may also be charged to comply with requests for further copies of the same information. This does not apply for all subsequent access requests.

Any fees applied must be justifiable and based on the administrative cost of providing the information.

Information must be provided to the Data Subject without delay and at the latest within one month of receipt. An extended period of compliance may be applied by a further two months where requests are complex or numerous. If this is the case, the Council must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

In the event of receiving a very general Data Access Request, e.g. "please give me everything you have on me", additional information may be sought on the nature of the request, such as the approximate date of a particular incident, our reference number, the identity of the other party, etc.

Where the data relates to information managed by a Data Processor, the council shall work with the external provider to source the requested information.

Where the Data Protection Officer refuses to respond to a request, they must provide a justification to the individual, informing them of their right to complain to the Office of the Data Protection Commission without undue delay and at the latest within one month.

Requests by the Garda Síochána

The policy and procedure in relation to requests by the Garda Síochána (or other law enforcement or investigation agency) for access to data from council records in relation to the prevention, detection or prosecution of offences or investigations of incidents is that any such request should:

- Be made in writing and include the PULSE reference number
- Provide detail in relation to the data required.
- State the reason it is required.
- Quote the relevant legislation which applies to their request for data.
- Be signed by a person at management level in the organisation, e.g. Garda Sergeant in Charge, Investigating Manager etc.

Exemptions to the Right of Access

The Data Protection Acts provides that individuals do not have a right to see information relating to them where any of the following circumstances apply.

- If the information is kept for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders, or assessing / collecting any taxes or duties: but only in cases where allowing the right of access would be likely to impede any such activities.
- If the information concerns an estimate of damages or compensation in respect of a claim against the council, where granting the right of access would be likely to harm the interests of the organisation.
- If the information would be subject to legal professional privilege in court.
- If the information is kept only for the purpose of statistics or carrying out research, but only where the information is not disclosed to anyone else, and where the results of the statistical work or research are not made available in a form that identifies any of the individuals involved
- If the information is back-up data. (NOTE: back-up data is not necessarily the same as old or archived data. Such archive data is subject to an individual's right of access in the normal way).
- A Data Protection Officer is not obliged to comply with an access request if that would result in disclosing data about another individual, unless that other individual has consented to the disclosure. However, the Data Protection Officer shall disclose so much of the information as can be supplied without identifying the other individual by redaction of names or particulars.
- Where personal data consists of an expression of opinion about the Data Subject by another person, the Data Subject has a right to access that opinion except if that opinion was given in confidence. If that opinion was not given in confidence, then the possible identification of the individual who gave it does not exempt it from access.

10. Data Protection by Design and by Default

Data protection needs to be at the heart of all future projects as set out in article 25 of the GDPR. A DPIA is the process of systematically considering the potential impact that a project or initiative might have on the privacy of individuals. It will allow organisations to identify potential privacy issues before they arise and come up with a way to mitigate them. A DPIA can involve discussions with relevant parties/stakeholders. The GDPR introduces mandatory DPIAs for those organisations involved in high-risk processing; for example where a new technology is being deployed, where a profiling operation is likely to significantly affect individuals, or where there is large scale monitoring of a publicly accessible area.

Fingal County Council will also adopt privacy by design as a default approach; privacy by design and the minimisation of data have always been implicit requirements of the data protection principles. However, the GDPR enshrines both the principle of 'privacy by design' and the principle of 'privacy by default' in law.

This means that Fingal County Council will ensure that the service settings they provide will be privacy friendly, and the development of services and products will take into account privacy considerations from the outset.

11. Staff Education and Training

The Council shall identity the education and training requirements of staff to help ensure that the Council complies with legislation and best practice when handling personal information. Staff at all levels shall be adequately trained to understand their responsibilities when processing the personal data of others.

All reasonable measures should be taken to ensure that staff are made aware of the organisation's data security measures and that staff are complying with them. All staff shall receive training at induction, and on a periodic basis, in accordance to their role, to ensure their awareness of the data protection requirements. The training shall include:

- their obligations in respecting and ensuring appropriate data protection within the Council;
- the need for data privacy.
- how to recognise data security breaches and what to do in the event of a data security breach.
- expertise available to advise on queries and subject access requests when received

All staff shall undertake training in data protection, confidentiality, IT/cyber security, with additional training for the Information and Data Management Team.

The Council shall ensure that Information and Data Management Team has an appropriate level of expertise in data protection law and practices to enable them to carry out their critical role, including the ability to support Subject Access Requests.

The Council's Data Protection Office is the primary point of contact for the public wishing to make Data Subject Access Requests as well as for contact by the Office of the Data Protection Commission.

12. Policy review and other relevant documents

It is the policy of Fingal County Council to review this policy periodically in light of its operation and in terms of new legislative or other relevant factors and following guidance from the Office of the Data Protection Commission.

All other relevant policies, templates and statements related to data protection are available on the Council website at https://www.fingal.ie/council/service/data-protection . All data protection policies, templates and statements are subject to regular review.

Document Control

Document Ref:	FCC/GDPR/POL/001	**Title:**	Data Protection Policy
Version& Date:	26/10/2018	**Author:**	Colm McQuinn, DPO
Directorate:	Corporate Affairs & Governance	**Department:**	
		Approved by Management Team on:	**03/12/2018**
Reviewed:	**03/11/2021 22/04/2022**	**Changes Approved by:**	**EMT**
		Date:	**22/04/2022**