Comhairle Cathrach & Contae Phort Láirge
Waterford City & County Council

Data Protection Policy

Contents

Chapter 1

Introduction

Introduction

Data Protection is the means by which the privacy rights of individuals are safeguarded in relation to the processing of their personal data.

Waterford City & County Council ("the Council") is the democratically elected organisation that governs the administrative area of Waterford City and County. The principal function of the Council is to provide a wide range of services to citizens under the following main headings:

- Housing and Building
- Roads, Transportation and Safety
- Water and Sewage
- Development Incentives and Controls
- Environmental Protection
- Recreation and Amenity
- Agriculture, Education, Health and Welfare
- Economic and Community Development
- Cultural and Library Services
- Miscellaneous

In performing its functions, the Council processes significant amounts of personal data and must comply with the EU General Data Protection Regulation ("GDPR") and the Data Protection Acts 1988 -2018 ("the DPA") – known collectively in this policy as "the Data Protection Acts.

The Data Protection Acts confer rights on individuals as well as responsibilities on those whose process personal data.

Purpose

The purpose of this document is to outline the Council's policy for fulfilling its obligations under the DPA. It sets out responsibilities for all managers, employees, contractors and anyone else who can access personal data in the course of their work for the Council.

Definitions (See Appendix 1 for details on the terms used in this Policy)

Scope

What information is covered by this policy?
This policy applies to all personal data created or received in the course of Council business in all formats, of any age. Personal data may be stored or transmitted in paper, physical and electronic formats or communicated verbally in conversation or over the telephone.

To whom does this policy apply?
This policy applies to:

- All employees of the Council ("employee" includes paid or unpaid work placements, graduates, interns, community employment scheme workers etc) who process personal data in the course of their employment or placement; and

- Individuals not directly employed by the council but who are employed by contractors (or subcontractors) and who process personal data on behalf of the Council.

Where does the policy apply?
This policy applies to all locations where Council personal data is accessed, at the workplace, in the field and home use.

Chapter 2

Data Protection Policy
It is the policy of Council to ensure that processing of personal data will be governed by the principles of the DPA:

- Lawfulness, Fairness and Transparency;
- Purpose Limitation;
- Data Minimisation;
- Accuracy;
- Storage Limitation;
- Integrity and Confidentiality;
- Accountability.

In addition, the Council commits to the following:

- The rights of data subjects are fully respected and protected;
- Policies and procedures are in place to respond appropriately to personal data breaches ;
- A culture of respecting data privacy is promoted throughout the organisation;
- Appropriate data protection training and development is delivered to all members of management and staff;

Lawfulness, Fairness and Transparency
The Council is committed to ensuring that the personal data it collects from data subjects is obtained lawfully, fairly and in a transparent manner. At the time it collects personal data from data subjects or, in instances where data is obtained from a third party, as soon as practical and before the commencement of processing of such data, the Council will make data subjects aware of the following:

- Who is collecting the personal data (eg. Housing section of WCCC);
- Why it being collected;
- What legal basis is being relied upon to process the data (eg. Housing Acts, Planning Acts);
- How it will be processed;
- How long it will be kept for; and
- Who it will be disclosed to.

Data Protection Notices will be developed for the various sections of the Council to ensure this requirement is met.

Lawful processing conditions for personal data are as follows:

- The data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- The processing is necessary for compliance with a legal obligation to which the Council is subject;
- The processing of the personal data is necessary in order to protect the vital interests of the data subject or of another natural person;
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority which is vested in the Council; and
- The processing is necessary for the purposes of the legitimate interests pursued by the Council or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

In instances where the Council is relying on **consent** as a lawful processing condition the data subject's consent must be freely given, unambiguous, specific, informed and given though a clear and affirmative action. Data subjects must be informed, at the time of the giving of consent, of their right to withdraw consent at anytime.

Special categories of personal data (see definition in Appendix 1) are subject to additional protection. In accordance with Section 45 of the Data Protection Act 2018, processing of special categories of personal data shall be lawful to the extent that processing is

a) Authorised by Section 41 and Sections 46 to 54 of the Data Protection Act 2018 or
b) otherwise authorised by Article 9 of the GDPR.

Purpose Limitation

The Council will, except where otherwise provided by data protection legislation, take measures to ensure that the processing of personal data is limited to the purposes for which it was obtained. Disclosures of personal data to third parties will only occur in circumstances that are permitted by law.

Data Minimisation

The Council will put in place appropriate measures to ensure that the personal data held by it is proportionate for the specified purpose that it was obtained. The personal data collected should be adequate and not excessive for the specified purpose. Consequently all application forms and other means that are used to capture personal data will be designed

so that they capture the minimum amount that is necessary to achieve the specified purpose.

Accuracy
The Council must ensure that the personal data being processed is accurate and where necessary, kept up to date. Procedures will be put in place to ensure high levels of personal data accuracy, including periodic review and audit.

Storage Limitation
Waterford City & County Council will retain personal data for no longer than is necessary. Retention periods will be determined by reference to the National Retention Policy for Local Government Records issued by the Local Government Management Agency (LGMA).

Integrity & Confidentiality
The Council will maintain the highest standards of technical and organisational security measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network. Security measures will be designed in such a manner that they are proportionate to the risks and sensitivities associated with the various categories of personal data that are under the control of the Council.

The Council shall ensure that it will, where processing is carried out on its behalf, choose a processor that provides sufficient guarantees in respect of the technical and organisational security measures that are required to protect personal data.

Accountability
The principal of accountability creates a positive duty on the Council to actively monitor and manage the processing of personal data and to demonstrate compliance with the Data Protection Acts. The Council will develop a range of organisational wide policies, procedures and practices to underpin data protection compliance and will implement appropriate monitoring and reporting mechanisms.

Data Subject Rights
Data subjects have a range of rights under the Data Protection Acts. These include the following:

- The right to be informed;
- The right of access;
- Right to rectification of inaccurate or incomplete data;
- The right to erasure of personal data (also known as the 'right to be forgotten');
- The right to portability;
- The right to object to the processing of personal data;

- The right to restrict the processing of personal data; and
- Rights in relation to automated decision making, including profiling.

The Council will develop appropriate policies and procedures to assist data subjects to avail of these rights.

Personal Data Breaches

The Council will take all precautions to prevent personal data breaches. In the event of a personal data breach occurring appropriate measures will be in place to ensure necessary steps are taken including:

- The identification of personal data breaches and their consequences;
- The notification of personal data breaches where required;
- Limiting and / or remedying the impact of personal data breaches; and
- Implementing controls to prevent a reoccurrence of the personal data breach.

Policies and procedures are in place within the Council to ensure appropriate response to personal data breaches.

Privacy by Design & by Default

Privacy by design and the minimisation of data have always been implicit requirements of the data protection principles. GDPR now enshrines both the principle of 'privacy by design' and the principle of 'privacy by default' in law. This means that service settings must be automatically privacy friendly, and requires the Council to take account of privacy considerations from the outset of any project (eg. any new form of data processing, changes to service provision, software development, IT systems). This will be achieved by carrying out DPIAs as required.

Data Protection Impact Assessments (DPIA)

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 the Council to identify potential privacy issues before they arise, and come up with a way to mitigate them. The Council will develop appropriate procedures in relation to DPIA and ensure they are carried out for relevant projects.

CCTV

All usage of CCTV, other than in a purely domestic context, must be undertaken in compliance with the requirements of the Data Protection Acts. All uses of CCTV must be **proportionate** and **for a specific purpose**. As CCTV (and other forms of covert surveillance for example for the purposes of preventing illegal dumping) can infringe the privacy of the persons captured in the images, there must be a genuine reason for installing such a system. If installing a CCTV system, the **purpose** for its use must be displayed in a prominent

position. Before installing any CCTV system or carrying out any forms of covert surveillance, the Data Protection Officer should be consulted and a Data Protection Impact Assessment must be undertaken.

Chapter 3

Roles & Responsibilities

The Council has overall responsibility for ensuring compliance with the Data Protection Acts. However, all employees who process personal data in the course of their employment are also responsible for ensuring compliance with the Data Protection Acts.

The Council will provide support, assistance, advice and training to all relevant departments, sections and staff to ensure they are in a position to comply with the legislation. The Council's Data Protection Officer (contact details below) will assist the Council and its staff in complying with the Data Protection legislation.

Specifically, the following roles and responsibilities apply in relation to this Policy:

All employees of the Council:

- Acquaint themselves with, and abide by, the rules of Data Protection set out in this policy;
- Read and understand this policy document;
- Understand what is meant by 'personal data' and 'special categories of personal data' and know how to handle such data;
- Understand the lawful basis for processing personal data;
- Must complete relevant training and awareness activities provided by the Council to support compliance with this policy;
- Should take all necessary steps to ensure that no breaches of information security result from their actions;
- Must report all suspected and actual data security breaches to their line manager who must in turn report the incident immediately to the Data Protection Officer so that appropriate action can be taken to minimise harm; and
- Contact the Data Protection Champion in their section and/or the Data Protection Officer if in any doubt.
- Must inform the Council of any changes to the information that they have provided to the council in connection with their employment (e.g. changes of address or bank account details).

Council Senior Management Team (SMT)

(Chief Executive, Directors of Service & Head of Finance)

- The SMT is responsible for reviewing and approving this policy as recommended by the Director of Corporate Services;
- Each member of SMT is responsible for ensuring compliance with the Data Protection Acts and this policy in their respective areas of responsibility; and

Director of Corporate Services

The Director of Corporate Services is the Senior Officer within the Council, with accountability for compliance with the Data Protection Acts and for:

- Ensuring that this Policy is reviewed and approved by the SMT as appropriate;
- Ensuring that appropriate policies and procedures are in place to support this Policy;
- Liaising with the SMT as appropriate;
- Leading the internal Information Security Team
- Ensuring that any data security breaches are properly dealt with.

Senior Managers
(Senior Executives Officers /Senior Engineers and equivalent)

- Driving and promoting a culture of good data management and information security within all areas of work under their control;
- Ensuring staff are fully aware of their responsibilities under the data protection legislation;
- Ensuring that all policies and procedures relating to data protection and information security are complied with in all areas of work under their control;
- Ensuring that any data breaches are detected, reported and responded to as quickly as possible and in line with the Council's policy and procedures and in conjunction with the Data protection Officer;
- Taking a lead role in investigating any serious data breach within their area of work;
- Nominating a suitable member of staff to be responsible for coordinating Data Protection compliance matters within each of the areas under their remit – this staff member ("Data Protection Champion") will participate in the organisational GDPR working group;
- Ensuring that a record of processing activities ("Register of Personal Data") is compiled and maintained for their areas of responsibility;
- Approving and returning the information required for the compilation of the Council's Register of Personal Data to the Data Protection Officer;
- Ensuring a Data Protection Impact Assessment (DPIA) is carried out where appropriate for any new projects within their area of work; and
- Ensuring a process is in place within their area of work to respond within timeframes to a Data Subject Access Request (DSAR).

Data Protection Officer

The Data Protection Officer is responsible for administrative matters at an institutional level in relation to data protection. The principal data protection duties of the Data Protection Officer are to:

- Provide advice and guidance to Council staff on data protection matters;
- Act as the contact point for and cooperate/liaise with the Data Protection Commission where necessary/appropriate, including in the event of a data security breach;

- Work with Human Resources (HR) to organise targeted training and briefing sessions for Council staff and elected members as required;
- Act as point of contact for formal Data Access Requests and work with the Data Protection Champions to process and respond to same;
- Respond to requests for rectification, erasure of data and restrictions or objections to processing of data;
- Initiate regular reviews of data protection policies and procedures and ensure documentation is updated as appropriate;
- Provide advice to staff in relation to the completion/outcome of Data Protection Impact Assessments;
- Maintain a centralised register of the categories of personal data ("Council's Register of Personal Data");
- Maintain a centralised register of all 3rd party data processors and monitor their compliance with data protection obligations;
- Maintain a centralised record of all personal data security breaches;
- Maintain records of the Council's compliance with the Data Protection Acts;
- Maintain a list of and provide support to the nominated Data Protection Champions within each area of the Council with responsibility for coordinating data protection matters within their own areas.
- Report quarterly to the Chief Executive on all Data Protection matters

Data Protection Champions

Each section of the Council which processes personal data is required to nominate a suitable member of staff to be responsible for coordinating Data Protection compliance matters within their respective area, such matters to include:

- Being a point of contact for the Data Protection Officer regarding all data protection related matters;
- Compiling and maintaining the information required from their area for the Council's Register of Personal Data;
- Bringing relevant Data Protection/IT security matters to the attention of relevant staff in his/her area;
- Participating in training in data protection/IT security where appropriate and
- Co-ordinating the response (in conjunction with the Data Protection Officer) to any Data Subject Access Requests.

Other individuals /contractors processing personal data on behalf of the Council:

All other individuals/contractors who process personal data are expected to:

- Acquaint themselves with, and abide by, the rules of Data Protection set out in this policy;
- Read and understand this policy document;
- Understand what is meant by 'personal data' and 'special categories of personal data' and know how to handle such data;
- Understand the lawful basis for processing personal data;

- Not jeopardise individuals' rights or risk a contravention of the Act;
- Report all data security breaches immediately; and
- Enter into a Data processing Agreement /Confidentiality Agreement with the Council where required

Compliance with the Data Protection Policy

Failure by any employee to comply with the terms of this Data Protection Policy may result in disciplinary procedures in line with the Council's Disciplinary Procedure.

Failure by any contractor (or sub contractor) or any other individual processing personal data on behalf of the Council to comply with the terms of this Data Protection Policy may result in termination of that contract.

Supporting Policies, Procedures & Guidelines

This policy supports the provision of a structure to assist in the Council's compliance with the Data Protection Acts. The policy is not a definitive statement of Data Protection law. Any specific queries should be referred to the Council's Data Protection Officer.
(see contact details below).

The Policy should be read in conjunction with the following Council policies, procedures and guidelines:

Data Protection:

- Data Subject Access Request procedure
- Personal Data Breach Notification –Guidance Notes
- Data Privacy Impact Assessment (Template)

Records Management

- Waterford City & County Council Records Management Policy & Procedures
- National Retention Policy for Local Government Records
- Clean Desk Policy

IT security & related

- Suite of IT Security Policy & Procedures (to be revised/developed)

Training and Development

- The Council will provide data protection and information security training for all staff at a level appropriate to their role and responsibilities.
- Data protection and information security training will be covered as part of induction for all new staff.
- Ongoing refresher training will be organised as required but at least once a year.

- Data Protection training will be provided for elected members on a regular basis but in particular after first election/co-option onto the Council

Monitoring and Review

This policy document will be subject to on-going monitoring and review.

Further Information

Further information and advice on the operation of this policy document is available from the Council's Data Protection Officer.

Contact details:
Phone: 0761 10 20 20
E-mail: dataprotection@waterfordcouncil.ie
Website: www.waterfordcouncil.ie
Postal Address: Data Protection Officer,
Waterford City & County Council, City Hall, Waterford X91 PK15

Appendix 1 Definitions

For the purposes of this policy document the following definitions apply:

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. (*Waterford City & County Council is the Data Controller in relation to processing of personal data for customers and employees)*

Data Subject: is an individual who is the subject of personal data *(can be a customer, employee or supplier; can be a member of the public whose image is captured on CCTV)*

Data owner: is the most senior person in the section within which the data is created. An exception can be made if this role has been explicitly and formally delegated to someone else by the most senior person in the aforementioned areas. Data owners have overall responsibility for the quality and integrity of the data held in their area.

Personal Data: any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Note: While the Data Protection legislation only applies to data relating to LIVING individuals, the Council will also give due care and attention to personal/sensitive data relating to deceased individuals.

Registers of Personal Data: In order to maintain documentation on processing activities, the Council will create a central Register of Personal Data which documents what personal data we hold as a Data Controller, what we use it for, the legal basis we are relying on in order to process the data, who we may share it with, where it is held and how long we keep it.

The Council is also required to hold a register of personal data it holds where it acts as a **data processor**.

Every section in the Council is required to record the information required to compile the Registers. This process will be coordinated by the Data Protection Officer. Nominated Data Protection Champions are responsible for co-ordinating the compilation of the required information for their own area, in consultation with their line manager/ section head. Senior managers must ensure the required information is returned to the Data Protection

Officer; they must also ensure that the data protection Officer is notified with details of any changes to the processing of personal data carried out in their area.

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

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.

Processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of Waterford City & County Council.

Special Categories of Personal Data: is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; genetic data; biometric data processed for the purpose of uniquely identifying a natural person; data concerning health and data concerning a natural person's sex life or sexual orientation.

Appendix 2 – Examples of Personal Data

Examples of Personal Data (not an exhaustive list)
People's names
Contact Details (incl. Home address, home phone/mobile nos., email addresses
Date of Birth/Age
Marital Status
Next of kin / dependent / family details
Birthplace/citizenship/nationality
Gender
Data concerning a person's sex life or sexual orientation
Data Concerning health
Data relating to children
PPS Numbers
Personal financial data (e.g. Bank account details, credit card Nos.)
Income / salary
Car registration details
Photographs
CCTV / Video images containing identifiable individuals
Voice recordings
Online identifiers (e.g. IP address)
Employee Nos.
Staff ID cards
Passwords & PINS
Sick leave details/medical certificates
Other leave data (excl. sick leave)
Grievance/Disciplinary Details
Performance Development Plans (PDPs) & other work performance documents
Membership of Professional Associations
CVs (including Qualifications/Education Details & references)
Employment History

Special Categories of Personal Data
Racial or Ethnic origin
Political opinions
Religious or philosophical beliefs
Membership of a trade union
Data relating to the commission or alleged commission of any offence (incl. Garda vetting data)