DUN LAOGHAIRE-RATHDOWN COUNTY COUNCIL

Comhairle Contae County Council

DATA PROTECTION POLICY

Dun Laoghaire-Rathdown County Council

1. INTRODUCTION

Dun Laoghaire-Rathdown County Council is the local authority for the County of Dun Laoghaire-Rathdown ("the Council") and it is responsible for the provision of a range of services to meet the social, economic and cultural needs of 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 of Dun Laoghaire-Rathdown, 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 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, the Council may be required from time to time to collect, process and use certain types of personal data to comply with its regulatory or legislative requirements.

The Council is obliged to comply with the obligations contained in the GDPR and the Data Protection Act 2018 (DPA) in relation to the processing of personal data.

PERSONAL DATA AND SPECIAL CATEGORIES OF PERSONAL DATA

"Personal data" means any information relating to an identified or identifiable natural person (who is known as the 'data subject' in GDPR). In practice, any data about a living person who can be identified from the data will constitute personal data. Examples of personal data can be found in Appendix D.

Stronger safeguards are required for **special categories of personal data** (previously known as sensitive personal data). The following are special category personal data:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Data concerning health
- Data concerning a person's sex life or sexual orientation
- Genetic data

- Biometric data

Data concerning health is the most common special category personal data processed by the Council (e.g. processing of disability grants and health information furnished with housing applications). Data concerning health means personal data relating to the physical or mental health of an individual, including the provision of health care services to the individual, that reveal information about the status of his or her health.

Data identifying people from the travelling community (ethic origin) or details of employee trade union membership may also be processed by the Council from time to time.

Special category personal data can only be processed under specific circumstances.

Personal data relating to criminal convictions and offences, while not included in the list of 'special categories' of personal data, have extra safeguards applied to processing them. See Appendix C.

Please see the Definitions section of this Policy for details on the terms used on this policy.

2. PURPOSE

This policy is a statement of the Council's commitment to protect the rights and privacy of individuals in accordance with the GDPR and the DPA. It sets out responsibilities for all managers, employees, contractors and anyone else who can access or use personal data in their work for the Council. If any person has any question about the contents of this policy, please contact the Council's Data Protection Officer whose contract details can be found in Section 11 below.

3. SCOPE

3.1. What information applies to this policy?

This policy applies to all personal data processed by the Council in the course of its business in all formats and of any age. Personal data may be held or

transmitted on paper, electronically or may be communicated verbally in conversation or over the telephone.

3.2 To whom does this policy apply?

This policy applies to:

- any person who is employed by the Council who uses personal data in the course of their employment;
- Contractors or service providers who process personal data in the course of their engagement with the Council

3.3 Where does this policy apply?

This policy applies to all locations from which personal data in the control of the Council is processed, including the processing of personal data from remote locations.

4. POLICY

The Council undertakes to process data in accordance with the GDPR and the DPA.

4.1. PRINCIPLES RELATING TO THE PROCESSING OF PERSONAL DATA

The Council is responsible for, and must be able to demonstrate, compliance with the following data protection principles:

Personal data shall be:

(a) Processed lawfully, fairly and in a way that is transparent to the data subject **("lawfulness, fairness and transparency")**

(b) Collected, created and processed only for one or more specified, explicit and lawful purpose(s) **("purpose limitation")**

(c) Adequate, relevant and limited to what is necessary for those purposes **("data minimisation")**

(d) Accurate and, where necessary, kept up to date **("data accuracy")**

(e) Retained for no longer than necessary **("storage limitation")**

(f) Kept safe and secure **("integrity and confidentiality")**

These principles are binding on the Council as a **'data controller'.** A failure to comply with these principles constitutes a breach of the GDPR. A further explanation of the data protection principles is outlined below:

A. Process personal data lawfully, fairly and transparently

Legal Basis for Processing

In order for the Council to collect and process personal data "lawfully", the Council must have a legal basis for doing so. There are six available legal bases for processing as follows:

- **Consent:** the individual has given clear consent to the data subject to process their personal data for a specific purpose;
- **Contract:** the processing is necessary for a contract the data controller has with a third party;
- **Legal obligation:** the processing is necessary for the data controller to comply with the law;
- **Vital interests:** the processing is necessary to protect someone's life;
- **Public task:** the processing is necessary for the data controller to perform a task in the public interest or for its official functions;
- **Legitimate interests:** the processing is necessary for the legitimate interests of the data controller (Public bodies cannot avail of this legitimate interest legal basis and therefore this lawful basis cannot be used by the Council)

In respect of almost all of its processing of personal data, the Council will rely on its legal obligations under statute or that the processing is necessary for a contract that the Council has entered into as the lawful basis for processing of personal data. The specific legal basis (with reference to the specific section of relevant legislation or contract) must be identified in respect of each type of processing of personal data. Consent is not used as a lawful basis in respect of the Council's legal obligations under statute. The Council will use only use consent as a lawful basis for the processing of personal data as a last resort.

Processing of personal data must be done in a transparent manner

When the Council processes a person's personal data, it has to make certain information available to the data subject. This applies whether the information is collected directly from the individual or from another source. This information must be provided via a **'Privacy Notice'.**

PRIVACY NOTICES

When is a Privacy Notice required?

- Where information is being collected directly from an individual, a Privacy Notice must be provided at the point at which the data is collected. This includes Council forms where personal data is collected from the Council's service users.
- Where information is obtained from another source, a Privacy Notice must be provided:
  - at least one month after obtaining the data;
  - if personal data is to be used to communicate with the data subject at the latest at the time of the first communication with the data subjects
  - if disclosure to another recipient is envisaged, at the latest when personal data is first disclosed

What needs to be included in a Privacy Notice?

Privacy Notices must contain specific information which informs data subjects of:

- who is collecting the data (e.g. Housing Section, Dun Laoghaire-Rathdown County Council);
- why it is being collected (e.g. for the purpose of social housing allocation);
- what legal basis is being relied upon to process the data (e.g. the relevant section of the Housing Acts);
- how it will be processed (e.g. by way of manual forms/electronically);
- how long it will be kept for (as per the relevant retention schedule);
- who it will be disclosed to (i.e. to other departments within the Council or to other State Bodies)
- The lawful basis for the processing and the consequences of failure to provide the data;

What rights people have in relation to their own data (see section 5.6 relating to data subject rights below)

Individuals must also be made aware of:

- the right to lodge a complaint with the Data Protection Commission;
- the existence of automated decision making, including profiling

Each section of the Council is required to consider what Privacy Notices are required in respect of the personal data processed by that section. The Council is currently developing a Privacy Notice Procedure.

B. Process personal data only for one or more specified, explicit and lawful purposes *("purpose limitation")*

The Council, its contractors and service providers must:

- only keep personal data for purposes that are specific, lawful and clearly stated (i.e. as outlined in the relevant privacy notice);
- only process personal data in a manner which is compatible with these purposes;
- treat people fairly by using their personal data for purposes and in a way they would reasonably expect;
- ensure that the data is not reused for a different purpose that the individual did not agree to or would reasonably expect;
- ensure that the collection and processing of the data is lawful

C. Ensure that personal data being processed is adequate, relevant and not excessive *("data minimisation")*

The Council, its contractors and service providers should only collect the minimum amount of personal data from individuals that is needed for the purpose(s) for which it is kept (and referred to in the Privacy Notice).

Personal data should only be disclosed in ways that are necessary or compatible with the purpose for which the data is kept. Special attention should be paid to the protection of special categories of personal data, the disclosure of which would normally require one of the other specified lawful bases (see Appendix A).

D. Keep personal data accurate and, where necessary, up-to-date *("accuracy")*

The Council, its contractors and service providers must ensure that the personal data being processed is accurate and, where necessary, kept up-to-date.

E. Retain personal data no longer than is necessary for the specified purpose or purposes *("storage limitation")*

The Council, its contractors and service providers must be clear about the length of time for which personal data will be kept and the reason why the information is being retained. If there is no good reason for retaining personal data, then that data should be routinely deleted.

The Council, its contractors and service providers must comply with the Council's record management guidelines (available on the Communications Department Section of the Intranet) and apply the records retention schedules to keep records and information containing personal data only so long as required for the purposes for which they were collected. These guidelines require each section to put in place procedures to delete records in accordance with the records retention guidelines[1].

If the records management guidelines do not address the retention period for the personal data concerned, then it is necessary for the section to decide on an appropriate retention that is reasonable for the purposes for which the personal data was obtained.

GDPR allows for data to 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 subject to implementation of appropriate technical and organisational measures in order to safeguard the rights and freedoms of individuals.

F. Keep personal data secure *("integrity and confidentiality")*

Each section must take appropriate security measures to protect personal data from:

[1] Communications Department to confirm.

- unauthorised access;
- inappropriate access controls allowing unauthorised use of information;
- being altered, deleted or destroyed without authorisation;
- disclosure to unauthorised individuals;
- attempts to gain unauthorised access to computer systems e.g. hacking;
- viruses or other security attacks;
- loss or theft;
- unlawful forms of processing

While the GDPR does not specify the necessary security measures to be taken, they require that technological developments, the nature of the data and the degree of harm that might result from unauthorised or unlawful processing should be taken into consideration.

The Data Protection Commissioner has issued a guidance note on this security obligation and the Council will review its own security policies in light of this Guidance note.

When transferring personal data to a country outside the European Union, appropriate agreement and auditable security controls must be put in place to protect the personal data. Advice must be sought from the Council's Data Protection Officer in relation to any proposal for the transfer of personal data outside the European Union.

Accountability

The GDPR states that the Data Controller shall be responsible for, and be able to demonstrate, compliance with the above principles ("accountability"). This means that the Council must:

- maintain a record of all data processing activities (see 4.2. below);
- implement appropriate technical and organisational measures that ensure and demonstrate that we comply;
- implement measures that meet the principles of privacy by design and by default (see 4.3 below), such as:
  - data minimisation;
  - pseudonymisation;
  - transparency;
  - creating and improving security features on an ongoing basis

- use data protection impact assessments where appropriate (see 4.4 below);
- record all data security breaches (see 4.5 below)

4.2 RECORDS OF PROCESSING ACTIVITIES

Under article 30 of the GDPR and under section 81 of the DPA (relating to Law Enforcement functions), the Council is obliged to maintain a record of activities that involves the processing of personal data. This record of processing documents what personal data the Council holds as Data Controller, what the personal data is used for, the legal basis for processing the personal data, who the data is shared with, where it is held and how long it is retained for by the Council.

The GDPR Champion for each section has developed a record of processing (also referred to as data processing inventories) which has been signed off by the Senior Executive Officer in the relevant section. The inventory must be reviewed by the GDPR champions by the 31 January each year and signed off by the Senior Executive officer. Any changes to the record of processing must be reflected in an updated inventory with the changes expressly notified to the Data Protection Officer.

A separate record of processing must be maintained for the Council's Law Enforcement functions (i.e. planning enforcement, waste and litter enforcement, water pollution enforcement, air pollution enforcement).

4.3. PRIVACY BY DESIGN AND DEFAULT

Privacy by design and by default is written into Article 25 of the GDPR.

Privacy by Design states that any action an organisation undertakes that involves processing personal data must be undertaken with data protection and privacy in mind at every step. This includes internal projects, software development, IT systems, and much more. In practice, this means that the Council must ensure that privacy is considered during the whole life cycle of the system or process.

Privacy by Default means that once a product or service has been released to the public, the strictest privacy settings should apply by default, without any manual input from the end user. In addition, any personal data provided by the

user to enable a product's optimal use should only be kept for the amount of time necessary to provide the product or service. If more information than necessary to provide the service is disclosed, then "privacy by default" has been breached.

Council staff must apply the principles of Privacy by Design and by Default when processing any personal data by:

- Performing a Data Protection Impact Assessment (DPIA) - see section on DPIA's below - where data processing is likely to result in a high risk to the rights and freedoms of individuals, especially when a new data processing technology is being introduced;
- Performing a DPIA where required e.g. Installation of CCTV, large scale processing of special categories of data and personal data relating to criminal convictions;
- Collecting, disclosing and retaining the minimum personal data for the minimum time necessary for the purpose;
- Anonymising or pseudonymising of personal data wherever necessary and appropriate

4.4 DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

When the Council processes personal data, the individual whose data we are processing is exposed to risks. A DPIA is the process of systematically identifying and minimising those risks as early as possible. It allows the Council to identify potential privacy issues before they arise and come up with a way to mitigate them. All high risk processing such as the introduction of new CCTV, drone technology, body cams or dash cams and significant information technology projects require a DPIA to be prepared in advance. A DPIA will also be required prior to any tender process for goods or services which involves high risk processing, any data sharing proposals with other public bodies and for the introduction of any new IT systems.

The Council will develop a separate DPIA policy to provide information to assess whether a DPIA is required and guidance on how to conduct a DPIA.

4.5 PERSONAL DATA SECURITY BREACHES

A data protection breach occurs whenever personal data is subject to unauthorised disclosure, unauthorised destruction, lost or corrupted etc.

GDPR obliges the Council to notify the Data Protection Commission within **72 hours** after the Council becoming aware of a personal data breach. A data subject must also be notified where a breach constitutes a risk to the fundamental rights and freedoms of the data subject.

All members of staff must inform the GDPR champion for their section (or their substitute) of a personal data breach immediately on becoming aware of it. If a data breach is not notified to the Data Protection Commission within the 72-hour period, the Data Protection Commission has to be provided with reasons for not meeting this deadline.

The Council has developed a data breach procedure which should be followed in respect of all data breaches.

It is a matter for the GDPR champion for each section (or their substitute) to coordinate the response to a data breach and liaise with the Council's Data Protection Officer in accordance with the Council's data breach procedure which must be strictly followed in all cases. The GDPR champion (or their substitute) shall also be responsible for coordinating remedial action following any personal data breaches and for increasing awareness and education about the prevention of personal data breaches.

All personal data breaches shall be reported to the Senior Management Team and to the Privacy Programme Team and the Data Protection Officer shall maintain a log of all data breaches.

4.6. DATA SUBJECT RIGHTS

The GDPR provides rights for individuals, which are set out below. The Council's Freedom of Information Section (FOI Section) deals with all requests from individuals in relation to their rights. In the event that any member of staff receives a request from a member of the public in relation to their personal data, they should be directed to the FOI Section who will deal with the request.

The right to be informed

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR. See section above on Privacy Notices.

The right of access

Data subjects are entitled to make a Data Subject Access Request (DSAR) in writing under the Data Protection Acts for a copy of their personal data and for information relating to that data. This must be complied with within one calendar month. The one-month time period can be extended where the Council has received a number of requests or where the request of complex.

The Data Protection Co-Ordinator in the Freedom of Information Section will process all DSARs in accordance with the Council's Data Subject Access Procedure and they will keep a log of all DSARs. In certain circumstances, the Council is able to avail of exemptions from release of a person's personal data. In such cases, the exemptions will be interpreted strictly and the reasons for refusal will be logged by the FOI Section in the DSAR log.

The personal information of a data subject must not be disclosed to a third party, be they parent, potential employer, employer, professional body, etc. without the written consent of the individual concerned.

The right to rectification

The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete. An individual can make a request for rectification in writing. The Council must respond to a request within one calendar month. In certain circumstances, the Council can refuse a request for rectification.

All requests for rectification of personal data should be notified to the FOI Section without delay, who will advise further on the steps to be taken to response to the request.

The right to erasure

The GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as 'the right to be forgotten'. Individuals can make a request for erasure in writing. The Council must respond to a request within one calendar month.

All requests for erasure of personal data should be notified to the FOI Section without delay, who will advise further on the steps to be taken to respond to the request. In certain circumstances, the Council can refuse a request for erasure.

The right to restrict processing

Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances. When processing is restricted, the Council is permitted to store the personal data but not use it. An individual can make a request for restriction in writing and the Council must respond within one calendar month.

All requests to restrict the processing of personal data should be notified to the FOI Section without delay, who will advise further on the steps to be taken to response to the request.

The right to object

Individuals have the right to object to the processing of their personal data in certain circumstances. All objections to the processing of personal data should be notified to the FOI Section without delay, who will advise further on the steps to be taken to response to the request.

4.7. DATA PROCESSORS

The Council regularly engages third party service providers for the purpose of carrying out its services. Where the service involves the processing of personal data, it is necessary for the Council to enter into a data processing agreement as part of the contract with the service provider as the processing is being carried out on behalf of the Council by the service provider in accordance with the terms of the relevant contract. This data processing agreement imposes various obligations upon the service provider in relation to the personal data processed under the contract. Outside the obligations under a data processor agreement, data processors also have stand alone obligations under article 28 of GDPR.

The Council will develop a separate policy relating to data processors.

4.8. PERSONAL DATA RELATING TO CRIMINAL CONVICTIONS AND OFFENCES

The Council may be required to process personal data relating to criminal convictions and offences in the course of business and the provisions of GDPR apply to such processing. A lawful basis for processing this data must be identified. Whilst criminal conviction offences are not classed as special categories, GDPR provides additional rights to data subjects in this regard.

Garda vetting disclosures disclosed to HR must be secured with access to them by a restricted number of personnel only. A Garda vetting policy will be developed by the HR Department to ensure the adequate protection of personal data and any criminal convictions that are processed in line with that policy.

Where the Council processes personal data relating to criminal convictions and offences in its capacity as a regulator (i.e. where the Council is acting as a prosecutor with respect to planning prosecutions, litter prosecutions, water pollution prosecutions, etc.) the provisions of GDPR do not apply to the processing of personal data relating to criminal convictions and offences.
Instead, the Law Enforcement Directive which has been transposed into Part 5 of the Data Protection Act 2018 applies to the processing of this personal data. The requirements of the Law Enforcement Directive are broadly similar to the GDPR requirements, save for the transparency principle which means the Council does not have to inform data subjects what they are doing with a data subject's personal data by way of a Privacy Notice in the context of a criminal investigation or prosecution. Under section 81 of the DPA, a separate record for processing activity for personal data processed under the Law Enforcement Directive must be maintained (See section 4.2.)

4.9. PROFILING AND/OR AUTOMATED DECISION MAKING

Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a person, in particular to analyse or predict aspects concerning their performance at work or studies, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Advice and guidance on the GDPR implication of profiling and automated decision making must be sought from the Data Protection Officer in the event that profiling or automated decision making which involves the processing of personal data is being considered.

4.10. CCTV

The Council operates CCTV in respect of a number of its functions. The use of CCTV must be **proportionate** and for a **specific purpose.** A legal basis must be identified for the use of a CCTV system. The Data Protection Commissioner has released guidance on the use of CCTV systems which can be found on its website. Before installing a new CCTV system, staff from the relevant section must consult in advance with the Data Protection Officer and a DPIA has to be undertaken prior to any decision to install CCTV.

Where the Council uses CCTV for its Law Enforcement purposes, the use of such CCTV will be considered with reference to the relevant Law Enforcement functions.

The Council will develop a separate CCTV policy in relation to the use of CCTV.

4.11. USE OTHER VIDEO TECHNOLOGY THAT CAPTURES IMAGES OF INDIVIDUALS

In the event that the Council proposes to use body worn cameras, dash cams, automatic vehicle number plate recognition, drones or other technology that may capture or record images of individuals, staff from the relevant section must consult in advance with the Data Protection Officer and a DPIA has to be undertaken prior to any decision to operate such technology. A separate policy may have to be adopted for the use of such technologies.

4.12. DATA PROTECTION AND ELECTED MEMBERS

The Data Protection Commission has prepared guidance in relation to data protection in the context of dealing with representations from the Council's Elected Members and Members of the Oireachtas. This guidance can be found on the Data Protection Commission's website. As a result of this guidance, the Council will prepare a policy for data processing in relation to its dealing with the Elected Members.

4.13 COUNCIL EVENTS

The Council carries out a variety of events in the course of its business. Some of these events include photography or filming of persons. The Council will develop

a separate policy to cover the processing of such images of people at Council events.

4.14 COUNCIL'S INTRANET AND WEBSITE

The Council shall use the GDPR page on the Council's intranet as a forum in which to collate data protection policy and know-how for the benefit of staff of the Council.

The Council shall also ensure that its website provides detailed information of how the Council deals with its obligations under GDPR in respect of personal data processed by the Council.

4.15 CHILDREN'S PERSONAL DATA

Children are identified as "vulnerable individuals" and deserving of "specific protection". Any personal data that the Council processes relating to children must be afforded specific protection.

4.16 PROCUREMENT

Where the purchase of goods or services will involve the processing of special category personal data or involve the processing of a significant amount of personal data, a DPIA must be carried out prior to the issue of the tender for the goods and services. The Council's procurement policy will be amended to reflect this position.

4.17 DATA SHARING

The Council shares personal data with other public bodies for the purpose of carrying out its statutory functions. In all such cases the Council must enter into a data sharing agreement with the public bodies which sets out the responsibilities of each party in relation to the processing of personal data. In addition, a DPIA must be carried out prior to entering into any data sharing agreements with another public body.

5. ROLES AND RESPONSBILITIES

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

The Council will provide training and awareness activities to support staff in complying with GDPR. The Council's Data Protection Officer (contact details below) will also assist the Council and its staff in complying with the GDPR (Section 11).

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

COUNCIL'S MANAGEMENT TEAM

The Council's Management Team is responsible for approving this policy.

The Management Team shall be notified of all personal data breaches that occur within the Council and will also be notified of all significant issues relating to data protection.

DEPARTMENTAL CONTROLLER

Each Director of Service/Head of Function is the person responsible for complying with GDPR and driving a data protection compliance agenda in respect of the personal data processed within their Department and relevant sections within their Department. This responsibility may be delegated by the Director of Service/Head of Function to a person holding a Senior Executive Officer grade or analogous. The delegation of the responsibility of the Departmental Controller to the Senior Executive Officer or analogous shall provide for the following:

"All responsibilities in relation to Data Protection under the GDPR and the Data Protection Act 2018 in relation to the functions exercised by *[insert department]".*

The Departmental Controller in each Department/Section is responsible for taking steps to ensuring that their Department complies with GDPR in accordance with this policy and related policies and they shall work with the relevant Champion for this purpose.

Without prejudice to the general obligations of the Departmental Controller under GDPR and the DPA, the responsibilities of Departmental Controllers are as follows:

- To be responsible for compliance with this policy and the GDPR and DPA in respect of the processing of personal data in respect of the functions that are delegated to the Departmental Controller;
- To draw up an annual data protection compliance programme for their Department (in conjunction with the Data Protection Officer and other Departmental Controllers where appropriate)
- To ensure that that GDPR is a standing item on their Departmental team meetings.
- To work with their GDPR Champion in relation to GDPR matters and compliance arising out of the Privacy Programme Team agenda.
- To co-ordinate with other Departmental Controllers where necessary for the purpose of GDPR compliance.
- To update the Data Protection Officer on an annual basis on steps taken in their section in relation to GDPR compliance.
- To review and sign off on the record of processing activities by the 31 January each year (see section 4.2).

The Data Protection Officer shall be notified of the relevant Departmental Controllers within each Department/Section by the 31 January each year.

DIRECTOR OF CORPORATE, COMMUNICATIONS AND GOVERNANCE

The Director of Corporate, Communications and Governance shall be delegated with the responsibility for data protection policy. The Data Protection Officer and the Data Protection Co-ordinator shall support and advise the Director of Corporate, Communications and Governance in respect of this function.

Director of Corporate, Communications and Governance shall also be co-chair of the Privacy Programme Team.

DATA PROTECTION OFFICER

The tasks of the Data Protection Officer are designated in article 39 of the GDPR. The Data Protection Officer acts as an internal regulator in respect of GDPR compliance and is assisted with this function by the Data Protection Co-ordinator (details below).

The main roles of the Data Protection Officer are as follows:

- To provide information and advice to the Council, its staff and the Council's processors of their obligations under GDPR
- To monitor compliance with GDPR and with this policy, including the assignment of responsibilities and the training of staff
- To provide advice on Data Protection Impact Assessments
- To work with Internal Audit in relation to the carrying out of internal audits relating to GDPR compliance
- To provide advice on data protection policy.
- To deal with personal data breaches and maintain a log of breaches
- To be the contact point for the Data Protection Commission in relation to data breaches, investigations and audits
- To act as co-chair of the Privacy Programme Team (with the Director of Corporate, Communications and Governance)
- To support and advise the GDPR Champions
- To attend the LGMA Data Protection Officers network meetings (or send a substitute where he/she cannot attend the network meetings)
- To brief the Management Team on GDPR compliance

The Data Protection Officer in the performance of the above tasks must have regard to the risk of processing taking into account the nature, scope and context and purpose of the processing.

DATA PROTECTION CO-ORDINATOR AND THE FOI SECTION

The Data Protection Co-ordinator is the Senior Executive Officer in the Corporate, Communications and Governance Department and works with and provides support to the Data Protection Officer to ensure compliance with the Council's GDPR obligations. The Data Protection Co-ordinator will appoint members of the Freedom of Information section to assist in the delivery of the functions listed below. The Data Protection Officer and the Data Protection Co-ordinator shall meet on regular occasions to review matters relating to data protection.

The obligations of the Data Protection Co-ordinator are as follows:

- To manage the processing and response of Data Subject Access Requests (through the FOI Section)
- To manage the processing of all requests for rectification, erasure, restriction or objection to the processing of personal data
- To maintain a log of all DSARS and other requests
- To take steps to ensure that the Council enters into data processing agreements/data sharing agreements where appropriate and maintain a register of all data processing agreements/data sharing agreements.
- To work with the Data Protection Officer in relation to the provision of continuous staff training on GDPR
- To work with the Data Protection Officer in relation to data audits and investigations by the Data Protection Commission
- To attend the LGMA Data Protection Officers network meetings
- To be responsible for GDPR content on the Council's website
- To maintain a list of GDPR champions and substitutes
- To oversee the Secretariat support for the Privacy Programme Team

PRIVACY PROGRAMME TEAM

The Privacy Programme Team has been established to promote data protection compliance and learning throughout the Council.

The Privacy Programme Team is comprised of the Director of Corporate, Communications and Governance, the Data Protection Officer, the Data Protection Co-ordinator and GDPR Champions and their substitutes from the various sections of the Council. Departmental Controllers are also entitled to attend meetings of the Privacy Programme Team.

The Privacy Programme shall meet at regular intervals as determined by the Data Protection Officer and the Data Protection Co-ordinator from time to time.

The Minutes of the Privacy Programme Team shall be made available on the Council's intranet.

The Corporate, Communications and Governance Section shall provide secretariat support to the Privacy Programme Team.

GDPR CHAMPIONS

Each section of the Council shall have a GDPR champion and a substitute. A substitute shall undertake the role of the GDPR champion in the event that the GDPR Champion is unavailable. It is important to note that the GDPR Champion is not the primary person responsible for data protection in their section but instead they act as an advisor and point of contact on data protection matters for their relevant section.

The responsibilities of the GDPR Champions are as follows:

- To liaise with and support the Departmental Controller within their Department in relation to driving GDPR compliance and to assist in the production of a Data Protection Compliance plan fortheir Department/Section
- To be the point of contact for the Data Protection Officer in relation to personal data breaches
- To be the point of contact for the Data Protection Co-ordinator/Freedom of Information Section in relation to data subject access requests and other requests from data subjects
- To be the point of contact for all other data protection compliance matters and to assist the Data Protection Officer and Data Protection Co-ordinator where appropriate

INFORMATION TECHNOLOGY SECTION

The Information Technology section of the Council shall be responsible for providing advice on information technology security to ensure that the personal data processing by the Council is kept safe and secure and shall assist in developing a data protection security policy where necessary. The Information Technology Department shall ensure privacy by design and default is considered respect of any new Information Technology systems that are introduced by the Council.

INFORMATION SECURITY COMMITTEE

The Information Security Committee has been established to develop and maintain policies, procedures, and standards to ensure secure business practices are in place in the council. The Information Security Committee engages with the Information

Technology Section, providing oversight on a programme of work in relation to Information Security and Cyber Security initiatives. This will include work on the security of personal data processed by the Council.

The Information Security Committee is comprised of the Director of Corporate, Communications and Governance, the Data Protection Officer, the Data Protection Co-ordinator, the Head of IT and appropriate senior staff from the various sections of the Council.

INTERNAL AUDIT

Internal audit will undertake the role of a "third line of defence" in respect of the Council's GDPR obligations. The Data Protection Officer will liaise with the Internal Audit each year to decide on potential audits relating to GDPR compliance.

HUMAN RESOURCES

The Human Resources department shall be responsible for developing a training programme for staff in respect of data protection processing and compliance.

The Human Resources Department shall also be responsible for developing an appropriate induction module in respect of data protection for new staff who join the Council.

PROCUREMENT UNIT

The procurement unit of the Council shall adopt appropriate policies and procedures to ensure that data protection is considered in respect of the purchase or goods and/or services that involve the processing or personal data.

ALL STAFF OF THE COUNCIL

Staff of the Council are required to:

- Acquaint themselves and abide by this data protection policy
- Understand what is meant by "personal data" and "special categories of personal data".
- Understand what is meant by the lawful basis for processing personal data
- To protect individuals' rights under the GDPR and not to risk a contravention to the GDPR

- To report all personal data breaches to the GDPR Champion of their section immediately
- The contact the Data Protection Officer if in any doubt of their obligations under this policy or under GDPR

6. AWARENESS

The Council shall implement appropriate measures to makes its employees and other relevant parties aware of the content of this policy document.

7. SUPPORTING POLICIES, PROCEDURES AND GUIDELINES

This policy supports the provision of a structure to assist in the Council's compliance with the GDPR. However, it is not a definitive statement of data protection law. If you have any specific questions or concerns in relation to matters relating to personal data, please contact the GDPR Champion in your section or the Council's Data Protection Officer.

This policy should be read in conjunction with other policies and procedures and a list of such policies and procedures will be set on the GDPR page in the Council's intranet.

8. DEFINITIONS

PERSONAL DATA

Personal data means information relating to:

a. an identified living individual

b. a living individual who can be identified from the data, directly or indirectly, in particular by reference to:

- an identifier such as a name, an identification number, location data or online identifier, or
- one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual

This can be a very wide definition depending on the circumstances.

SPECIAL CATEGORIES OF PERSONAL DATA

Special categories of personal data (formerly known as "sensitive personal data") receive greater protection under the Data Protection Acts and refer to the following:

- racial or ethnic origin;

- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data or biometric data for the purpose of uniquely identifying a person;
- data concerning health;
- data concerning a person's sex life or sexual orientation

Data subjects have additional rights under Article 9 of the GDPR in relation to the processing of any such data.

Whilst criminal convictions and offences are not classed as special categories of personal data, the Data Protection Acts also provide additional rights to data subjects in this regard.

DATA SUBJECT

'Data subject' is a living person who is the subject of personal data.

DATA CONTROLLER

'Data 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. The Council is a data controller in relation to personal data of data subjects which it processes for the purpose of executing its statutory functions.

DATA PROCESSOR

'Data Processor' means a natural or legal person, public authority, agency or other body that processes personal data on behalf of a controller (Note: the term 'Data Processor' does not include an employee of a data controller who processes such data in the course of their employment). Examples of data processors include any service provider which the Council engages for the purpose of carrying out its statutory functions.

PROCESSING

'Processing' is widely defined under the GDPR. and means performing any operation or set of operations on personal data, whether or not by automated means, including:

- the collection, recording, organisation, structuring or storing of the data;

- the adaptation or alteration of the data;
- the retrieval, consultation or use of the data;
- the disclosure of the data by their transmission, dissemination or otherwise making the data available;
- the alignment or combination of the data; or
- the restriction, erasure or destruction of the data

DATA CONCERNING HEALTH

Data concerning health means personal data relating to the physical or mental health of an individual, including the provision of health care services to the individual, that reveal information about the status of his or her health.

PSEUDONOMYSATION

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. The GDPR still applies to personal data which has been pseudonymised.

9 REVIEW

This policy will be reviewed each by the Data Protection Officer. Any proposed amendments to this policy must be approved by the Council's Information Security Committee and notified to the Council's Management Team.

10 DATA PROTECTION OFFICER / DATA PROTECTION CO-ORDINATOR

The Council's Data Protection Officer is

Carmel Donlon
Data Protection Officer
Corporate Affairs Department
Dún Laoghaire-Rathdown County Council
E-mail: dataprotectionofficer@dlrcoco.ie

Feel free to contact her if you have any questions or suggestions in relation to this policy

The Council's Data Protection Co-ordinator is

Elizabeth Clarke
Data Protection Co-ordinator
Corporate Affairs Department
Dún Laoghaire-Rathdown County Council
Extension: 4268

Please contact Elizabeth if you have any queries in relation to data subject access requests.

E-mail: dataprotection@dlrcoco.ie

11. DISCLAIMER

The Council reserves the right to amend or revoke this policy at any time without notice and in any manner in which it considers fit at the absolute discretion of the Council's Management Team.

12. APPROVAL OF POLICY

This policy was approved by the Council's Management Team on the 12 November 2020. Any further changes to this policy require approval by the Council's Management Team or such other committee as delegated by the Council's Management Team.

Date: 28 May 2021

APPENDIX A:

LAWFUL BASES FOR PROCESSING (ARTICLE 6)

It is necessary under Article 6 of the GDPR to have a legal basis for processing all personal data. There are six legal bases set out in the legislation:

Consent from the individual

The individual must give consent at the outset. Inferred consent is not enough. Their consent must be freely given, and the withdrawal of their consent should not have any adverse consequences for the individual. As outlined on page 7 of this policy as a general rule the Council does not use consent as a lawful basis for processing personal data.

Necessary for the performance of a contract

The contract must be between the controller and the data subject and the data must be necessary for the performance of that contract or necessary in order to take steps to enter a contract with the data subject.

Necessary for compliance with a legal obligation

The Council is required by statute to retain certain records, for example employment records, health and safety records, student date. This lawful basis will cover a majority of the Council's data processing.

Necessary to protect the vital interests of the individual or another natural person

This ground is applied in essentially "life and death" situations, for example where it is necessary to provide personal data to the emergency services in the case of an emergency situation.

Necessary for the performance of a task carried out in the public interest

This may occur where the Council carries out a task in the public interest or in an exercise where official authority has been invested in the Council as a data controller. However, a data subject can object to this lawful basis and challenge whether the processing is indeed in the public interest.

Necessary for the legitimate interests of the controller or a third party

The processing is necessary for the Council's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. Public bodies such as the Council are not entitled to rely on legitimate interest as a lawful basis for the processing of personal data.

APPENDIX B:

CONDITIONS FOR PROCESSING SPECIAL CATEGORIES OF PERSONAL DATA (ARTICLE 9)

The GDPR sets out conditions for processing Special Categories of personal data. The Council must satisfy a lawful condition of processing personal data under Article 6 of the GDPR as well as under Article 9 to process these categories of data. The likely provisions of Article 9 shall will apply to the Council's processing of personal data is as follows:

- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.

- Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.

- Processing relates to personal data which are manifestly made public by the data subject.

- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

- Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to certain conditions and safeguards.

- Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

APPENDIX C:

CONDITIONS FOR PROCESSING PERSONAL DATA ABOUT CRIMINAL CONVICTIONS OR OFFENCES (ARTICLE 10)

The GDPR rules for sensitive (special category) data do not apply to information about criminal allegations, proceedings or convictions. The Law Enforcement Directive deals with personal data relating to criminal allegations, proceedings or convictions.

Instead, there are separate safeguards for personal data relating to criminal convictions and offences, or related security measures, set out in Article 10.

To process personal data about criminal convictions or offences, you must have both a lawful basis under Article 6 and either legal authority or official authority for the processing under Article 10. You must determine your condition for lawful processing of offence data (or identify your official authority for the processing) before you begin the processing, and you should document this.

The Data Protection Act 2018 deals with this type of data in a similar way to special category data, and sets out specific conditions providing lawful authority for processing it.

Article 10 also specifies that you can only keep a comprehensive register of criminal convictions if you are doing so under the control of official authority.

APPENDIX D:
EXAMPLES OF PERSONAL DATA *

The following is a list of the types of data which would be considered to be 'Personal Data'. **Please note:** this list is not exhaustive.

People's names

Contact Details (including home address, home phone/mobile numbers, e-mail addresses)

Date of Birth/Age

Birthplace/citizenship/nationality

Gender

Marital Status

PPS Numbers

Student/Staff Numbers

National ID Card details/Numbers

Next of kin / dependent / family details

Photographs with images of people

CVs

Personal financial data (e.g. Bank account details, credit card numbers)

Income / salary

Blood samples (linked to identifiable individuals)

Fingerprints

CCTV images of people

Voice recordings

Employment History

Sick leave details/medical certificates

Other leave data (excluding sick leave)

Qualifications/Education Details

Work performance

References for staff/students

Grievance/Disciplinary Details

Examination/assignment results

Membership of Professional Associations

Signatures (including electronic)

Passwords and PINS

Continuous Professional Development (CPD) records

Car registration details

Clinical files relating to research participants

Online identifiers (e.g. IP address)

Location data

Data relating to children

Research subject consent forms

SPECIAL CATEGORIES OF PERSONAL DATA:

Racial or Ethnic origin

Biometric data for the purpose of uniquely identifying a natural person

Political opinions

Data Concerning health

Religious or philosophical beliefs

Data concerning a person's sex life or sexual orientation

Membership of a trade union

Genetic data

Data relating to the commission or alleged commission of any offence (including Garda vetting data)

Any proceedings for an offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings