What is the purpose of this Data Protection Statement?

The Council is committed to meeting all relevant data protection, privacy and security requirements, whether originating from legal, regulatory or contractual obligations and is committed to protecting the rights and privacy of individuals in accordance with current data protection legislation. This statement should be read in conjunction with the GDPR and the Data Protection Acts.

This statement has been created to demonstrate the Council's commitment that the personal data you may be required to supply is in order to access services, will be processed in accordance with data protection principles, which state that personal data will be;

- Obtained lawfully, fairly and in a transparent manner
- Obtained for only specified, identified and legitimate purposes
- Processed for purposes which we have identified or purposes compatible with the purposes that we have identified
- Adequate, relevant and limited to what is necessary for purpose for which it was obtained
- Personal data collected and processed must be accurate and (where necessary) kept up to-date
- Kept only for as long as is necessary for the purposes for which it was obtained
- Processed in a manner that ensures the appropriate security of the personal data including protection against unauthorised or unlawful processing

High level statement implementation of GDPR Principles

The following is intended to provide a summary of activities of the Council to ensure that its management of personal data adheres with the principles of GDPR. These principles require that personal data shall be:

1) Processed lawfully, fairly and in a transparent manner.

The Council is developing a transparency programme to endeavour to ensure that at the earliest practical point in the collecting or processing of personal data that the individual is provided with written details, or made aware of how to access, a written statement of their privacy rights. We currently have a Privacy Statement that is available here.

2) Collected for specified, explicit and legitimate purposes

The Council processes personal data using a lawful basis as set out in Article 6 of the GDPR.

3) Adequate, relevant and limited to what is necessary for the purpose for which it was obtained

The Council endeavours to ensure that personal data sought is minimal and aligned to the purpose or activity for which it is required.

It should however be noted that 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 or to carry out functions in the public interest. This may extend to sharing or disclosure of personal data to other bodies to comply with our statutory obligations.

4) Accurate and, where necessary, kept up to date

The Council will provide reasonable opportunities for individuals to ensure personal data that is inaccurate can be deleted or corrected as required.
In practical terms this can often relate to changes in customers addresses and contact details. If you find that personal data we have about you is inaccurate or needs to be updated (for instance, you may have changed your name, address, contact details etc.) then please contact the Data Protection Co-ordinator (details at paragraph 6 below) so that we can correct it.

5) Kept only for as long as is necessary for the purposes for which it was obtained.

The National Retention Policy for Local Authority Records is under review. The revised Policy will provide information on the criteria for determining retention, archival and deletion or end dates for Council records in all the functions it operates.

6) Processed in an appropriate manner to maintain security

The Council, taking into account the nature, scope, purposes and related risks of processing, employ appropriate physical, technical and organisational measures to secure personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage. We also maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

- Confidentiality means that only people who are authorised to use the data can access it.
- Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.
- Availability means that authorised users should be able to access the data if they need it for authorised purposes.

In addition, the Council provides support, assistance, advice and data protection awareness training, which includes physical and IT security training for staff to ensure compliance with the legislation, and to ensure a secure environment for your personal data.

Compliance with GDPR and with the Data Protection Acts

The Council has designated a Data Protection Officer in accordance with requirements of the GDPR. Contact details are provided on the right hand side of this page. The Data Protection Officer's role is:

- to inform and advise the Council and the employees who carry out processing of their obligations pursuant to the GDPR;
- to monitor compliance with GDPR, regarding the policies of the Council in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
- to cooperate with the supervisory authority - the Office of the Data Protection Commissioner;
- to act as the contact point for the Office of the Data Protection Commissioner; on issues relating to processing, and to consult, where appropriate, with regard to any other matter.

Disclosure to third parties

It should be noted that staff of the Council may be required, from time to time, to collect process and use certain types of personal data to comply with regulatory or legislative requirements or to carry out functions in the public interest. This may extend to sharing or disclosure of personal data to other bodies to comply with our statutory obligations.

Typically, disclosure requests will involve requests from law enforcement/investigation agencies for purposes involving preventing, detecting or investigating offences, apprehending or prosecuting offenders or assessing or collecting any tax, duty or other monies owed or payable to the State, a local authority and/or to prevent injury or other damage to the health of a person or serious loss of or damage to property.

There are certain other limited circumstances where disclosures may be made.
Council officials who perform statutory duties involving preventing, detecting or investigating offences, apprehending or prosecuting offenders

or assessing or collecting any tax, duty or other monies owed or payable to the Council, may also access personal data where relevant to the performance of such duties. Access of this nature is confined to those staff performing such functions.

The Rights of the Data Subject

Individuals have the right to apply to:

- obtain from the data controller confirmation as to whether personal data concerning him or her are being processed, and, where that is the case, access to the personal data
- obtain from the data controller without undue delay rectification of inaccurate personal data concerning him or her
- obtain from the data controller the erasure of personal data concerning him or her without undue delay
- obtain from the data controller restriction of processing
- object, on grounds relating to his or her situation, to processing of personal data concerning him or her, in certain circumstances.

There are restrictions to these rights. The Council will examine each request to ensure that requests that can be granted are granted and where we are obliged to apply a restriction to a request, under the Acts, that we do so. On this basis general guidance on likely outcomes cannot be provided and requests from individuals seeking to exercise their rights will be assessed on a case-by-case basis against the various criteria to determine applicability. Full details of data subject rights and restrictions are outlined in Chapter 3 of the GDPR.

Please note that in respect of Data Subject Access Requests and other rights of the data subject as outlined in paragraph 6 please contact the Data Protection Co-Ordinator at:

Postal Address

Corporate, Communications and Governance Department
Dun Laoghaire-Rathdown County Council,
County Hall, Marine Road,Dun Laoghaire, Co Dublin. A96 K6C9.

Phone +353 1 205 4360
E-mail dataprotection@dlrcoco.ie

In relation to data subject access requests, we take steps to verify your identity before granting access to personal data. When making a data subject access request you will be asked to provide proof of your identity.

Data Protection Officer – Dun Laoghaire-Rathdown County Council

Our Data Protection Officer (DPO) advises and guides the staff of the Council in how they collect, use, share and protect your information to ensure your rights are fulfilled in compliance with the GDPR and Data Protection Acts. The DPO also acts as the contact point for individuals with concerns about the processing of their personal data and is also the liaison between the Council and the Office of the Data Protection Commissioner.

If you have any complaint about the processing of your personal data by the Council you may contact the Data Protection Officer at dataprotectionofficer@dlrcoco.ie. Please note that all requests for the access of your personal data should be made to the Data Protection Co-ordinator whose details are set out above.

Right of Complaint to the Data Protection Commissioner

If you are not satisfied with the outcome of the response received from the Council or the Council's DPO you are entitled to make a complaint to the

Data Protection Commissioner who may investigate the matter for you. The Data Protection Commissioner's website is www.dataprotection.ie or you can contact their Office at:

Postal Address Data Protection Commission, 21 Fitzwilliam Square South, Dublin 2, D02 RD28

Phone +353 578 648 800 or +353 761 104 800

E-mail info@dataprotection.ie

Statement on management of CCTV

The Council is developing a policy on the use of CCTV and details of the Council's CCTV Statement are here.

Security and Confidentiality

We protect your information with procedural, physical and technological measures and controls to ensure (in so far as it is possible) a safe and secure location for your personal data. The Council is committed to securing personal data through a range of measures aimed at minimising risks of the following outcomes relating to personal data.

- Alteration
- Loss
- Damage
- Unauthorised processing
- Unauthorised access.

In determining security measures, the Council first have regard to risks related to:

- the nature of the personal data (for example special category personal data should have less access and higher security arrangements);
- the context in which data is collected – for example whether there are risks related to how the data is collected – i.e. public areas etc.

Based on this assessment we then proceed to identify suitable organisational or technological options to address security, while having regard to the related cost of employing solutions.

Governance, Monitoring and Review

The Council has regard to the significant requirements under the GDPR and the Data Protection Acts and on this basis operates a governance structure to underpin compliance with its varied obligations.

Dun Laoghaire-Rathdown County Council will review this statement and supporting policies and actions periodically in light of its operation and in terms of new legislative or other relevant factors such as publication of guidance from the Office of the Data Protection Commissioner.