South Dublin County Council
Data Protection Compliance Guidelines

1. Purpose of Data Protection

The Data Protection Acts1988 to 2018 and the General Data Protection Regulation (GDPR) govern the processing of all personal data.

The purpose of the data protection legislation is to protect the privacy rights of living individuals regarding the processing of their personal data by those who control such data. In particular, it provides for the collection and use of data in a responsible way, ensures that such data must be safeguarded and is not used for purposes other than those specified at the time the data is collected.

2. Purpose of the compliance guidelines

The purpose of these procedures is to assist Council employees in supporting the Council's Data Protection Policy, which affirms its commitment to protect the privacy rights of individuals in accordance with the legislation. The guidelines set out the areas of work in which data protection issues arise, and outline best practice in dealing with these issues.

3. Explanation of terms

- **Data** means information in a form that can be processed. It includes both **automated data** and **manual data**.

- **Data subject** means an individual who is the subject of personal data.

- **Data breach** means 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.

- **Automated data** means any information on computer, or information recorded with the intention that it be **processed** by computer.

- **Manual data** means information that is recorded as part of a **relevant filing system** or with the intention that it forms part of a system.

- **Relevant filing system** means any set of information that, while not computerised, is structured by reference to individuals, or by reference to criteria relating to individuals, so that specific information relating to a particular individual is readily accessible.

- **Personal data** means data, including **sensitive personal data**, relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the Council.

- **Sensitive personal data** relates to specific categories of data, which are defined as data relating to a person's racial origin; political opinions or religious or philosophical beliefs; physical or mental health; sexual life; criminal convictions or the alleged commission of an offence; trade union membership.

- **Data controller** is a person or body that processes information about living people. The Data controller must be in a position to control the contents and use of a personal data file.

- **Data processor** is a person or body that processes personal data on behalf of a data controller.

- **Body** means an organisation, company and so on.

- **Processing** means performing any operation or set of operations on data, comprising:
    - obtaining, assembling, organising and storing data;
    - using, consulting and retrieving data;
    - altering, erasing and destroying data; or
    - disclosing data.
- **GDPR** is the General Data Protection Regulation.

4. Role of Data Protection Commission

The Data Protection Commission, with which the Council is registered as a data controller, oversees compliance with the terms of the legislation. The Commission has a wide range of enforcement powers, including investigation of Council records and record-keeping practices. A data controller found guilty of an offence can be fined up to €20 million and / or may be ordered to delete data.

5. Rules of Data Protection

There are eight rules of data protection, which govern the processing of personal data. When processing personal data the following procedures apply:

1. obtain and process the data fairly;

2. keep only for one or more specified and lawful purposes;

3. use and disclose only in ways compatible with the purposes for which it was initially given;

4. keep safe and secure;

5. keep accurate, complete and up-to-date;

6. ensure that it is adequate, relevant and not excessive;

7. retain no longer than is necessary for the specified purpose or purposes;

8. provide a copy of his / her personal data to any individual, on request.

In addition, there are special conditions that must be met before personal data may be transferred to a country outside the European Economic Area (E.U. member states and Iceland, Liechtenstein and Norway) if that country does not have an EU-approved data protection law. Specific provisions are in place concerning personal data transfers to the United States of America.

6. Application of the rules of data protection

In order to ensure compliance with these rules, staff must observe the following procedures at all times.

Obtaining and processing personal data

Personal data is obtained fairly if the data subject is aware of the purpose for which the Council is collecting the data and is provided with the following information:

● The Council's name and the particular business unit;
● Contact details of the Council's Data Protection Officer;
● Contact details of the Data Protection Commission;
● Service for which the personal data is required;
● Description of personal data required;
● Specific and legitimate purpose for which the personal data is required;
● Legal basis under which the personal data is required to be supplied;
● Other organisations / bodies / entities that the Council will be required to share data with, or obtain data from, in order to provide the required service;

● Details outlining how the personal data will be kept safe from unauthorised or unlawful processing;
● The period for which the personal data will be retained by the Council;

Data subjects **must** also be made aware of their **data protection rights** under the General Data Protection Regulation and Irish Data Protection Law as follows:
●To obtain confirmation as to whether personal data concerning the data subject is held;
●To request access to personal data held concerning the data subject;
●To be informed of the content and source of personal data held by the Council and to check its accuracy;
●To have inaccuracies corrected;
●To request the erasure of information;
●To object to direct marketing;
●To restrict processing of information, including automated decision making;
●To request data portability (transfer) of personal data held electronically by the Council to another data controller where technically feasible;
●To withdraw consent at any time where processing is based entirely on consent;
●To make a complaint to the Data Protection Commission;

The use of privacy notices specific to the service being provided is an effective means of advising data subjects of the required information and of their data protection rights.

Staff should obtain personal data only when there is a clear purpose for so doing, obtain only whatever personal data are necessary for fulfilling that purpose and ensure data are used only for that purpose.

Staff should obtain explicit consent in writing for processing sensitive data and retain a copy of the consent. Consent cannot be inferred from non-response in the case of sensitive data.

Council data processing facilities (including computers) should not be used by staff for capturing and storing personal data for non-work related purposes.

7. Disclosing personal data

Personal data should only be disclosed in ways that are necessary or compatible with the purpose for which the data are kept. Special attention should be paid to the protection of sensitive personal data, the disclosure of which would normally require explicit consent.

- Except where there is a statutory obligation to comply with a request for personal data, or where a data subject has already been made aware of disclosures, personal data must not be disclosed to any third party without the explicit consent of the data subject.

- Verbal consent to disclosure of personal data to the data subject may be obtained by telephone in the case of non-sensitive personal data, but must include asking the data subject to confirm a number of security details that should be known only to the data subject. The date and time of the giving of verbal consent should be recorded in writing.

- Disclosure of personal data to a third party is not permitted unless there is a statutory obligation to disclose, or the information is released, to the Gardaí for example upon receipt of a certified written request on headed paper, for the prevention of crime or investigation of an offence and if informing the subject of the disclosure would prejudice the enquiries, or unless it is in the vital interests of the data subject.

- Personal data should not be disclosed outside of the EEA unless written consent has been obtained, unless disclosure is required for the performance of a contract to which the data subject is a party, or unless disclosure is necessary for the purpose of legal proceedings.

8. Permitted disclosures of personal data other than to the data subject

The Acts provide for disclosures, other than to the data subject, where data are:

- required for safeguarding the security of the State;
- required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders, or assessing moneys due to the State or a local authority;
- required to protect the international relations of the State;
- required urgently to prevent damage to health or serious loss / damage to property;
- required under law;
- required for legal advice or legal proceedings;
- disclosed with the explicit consent of the data subject.

9. Data Access Requests

Data access requests must be directed to the Council's Data Protection Officer in the first instance. Requests must be processed within one month and in addition to the data requested replies to such requests must include the following information:

● Description of the purpose of, and legal basis for, the processing;

● Description of the categories of personal data concerned;
● Details of the recipients or categories of recipients to whom the personal data have been disclosed;
● Period for which the personal data will be retained, or where it is not possible to determine the said period at the time of the giving of the information, the criteria used to determine said period;
● Information detailing the rights of the data subject to request from the Council the rectification or erasure of the personal data concerned;
● Information detailing the rights of the data subject to lodge a complaint with the Data Protection Commission and the contact details of the Commission;
● Any available information as to the origin of the personal data concerned, unless the communication of that information is contrary to the public interest;

10. Securing personal data

The Council must protect personal data from unauthorised access when in use and in storage and the data must be protected from inadvertent destruction, amendment or corruption.

- Personal electronic data should be subject to appropriate stringent controls, such as secure passwords, encryption, access logs, backup, and so on.

- Screens, printouts, documents, and files showing personal data should not be visible to unauthorised persons.

- Personal manual data must be held securely in locked cabinets, locked rooms or rooms with limited access.

- Subject to retention guidelines, personal manual data should be destroyed by confidential shredding when the retention period has expired.

- When upgrading or changing a personal computer, staff should ensure the hard drive is cleaned by an appropriate ICT staff member.

- Special care must be taken where Council laptops and hand held devices containing personal data are used outside the Council offices.

- Council files and records must not be transferred to personal home computers or any other personal devices.

- Health and social work personal data can only be released following consultation with the relevant professional.

- Disclosing personal data to a Data Processor should be done only under a written contract specifying security rules to be followed.

11. Accuracy and completeness of personal data

Administrative procedures should include review and audit facilities so that personal data are accurate, complete and kept up-to-date.

12. Retention of personal data

Data should not be kept for longer than is necessary for the purpose for which they were collected. Data already collected for a specific purpose should not be subject to further processing that is not compatible with the original purpose. The Council's Record Management and Retention Policy document SDCC RECORD MANAGEMENT RETENTION POLICY FINAL 2 (003) (002).docx should be consulted for guidance on recommended retention periods.

13. Data Protection Impact Assessments

Preparation of a Data Protection Impact assessment is mandatory for all new high risk personal data projects initiated after the GDPR implementation date of 25th May 2018. An explanatory document has been provided by the Data

Protection Commission and is available on its website » Data Protection Impact Assessments (DPIA).

14. Personal Data Breaches

Notification of all data breaches which are likely to result in a risk to the rights and freedoms of data subjects must be reported to the Data Protection Commission **within 72 hours** and should be brought to the attention of the Council's Data Protection Officer **immediately**.

Reported breaches to the Data Protection Commission must include the following details:

- A description of the personal data breach, including, where possible, the categories and number, or approximate number, of data subjects concerned and the personal data records concerned
- A description of the likely consequences of the personal data breach
- A description of the measures taken or proposed to be taken by the Council to address the personal data breach, including any measures taken or proposed to be taken to mitigate its possible adverse effects
- The name and contact details of the Council's Data Protection Officer

Where a personal data breach occurs that is likely to result in a high risk to the rights and freedoms of a data subject whose personal data is breached , the data subject should be notified in writing of the personal data breach as soon as possible and such notification must include the following:

- A description of the nature and extent of the personal data breach
- A description of the likely consequences of the personal data breach
- A description of the measures taken or proposed to be taken by the Council to address the personal data breach, including any measures taken or proposed to be taken to mitigate its possible adverse effects
- The name and contact details of the Council's Data Protection Officer.

15. Disposal of personal data

Personal data should be securely disposed of when they are no longer needed for the purpose for which the data were collected nor for the effective functioning of the Council and its members. The method of disposal should be appropriate to the sensitivity of the data. Shredding is appropriate in the case of manual data and reformatting or overwriting in the case of electronic data. Particular care should be taken when personal computers are transferred from one person to another or outside the Council or are being disposed of.

16. Right of access to personal data by data subject

The Acts provide for the right of access by the data subject to his or her personal information. Data subjects must be made aware of how to gain access to their personal data. A data subject is entitled to be made aware of his or her right of access and to the means by which to access the data. A data subject is entitled to the following on written application within one calendar month:

- a copy of his or her personal data;
- to be informed of the content of personal data held by the Council;
- to be informed of the source of personal data held unless the communication of that information is contrary to the public interest;
- to be informed of the purpose of and legal basis for processing the personal data;
- to be informed of the right to have inaccuracies corrected and to request erasure of personal data;
- to be informed of the right to request restriction of processing of personal data, including automated decision making;

- to be informed of the right to withdraw consent at any time where processing is based entirely on consent;

- to be informed of the right to object to direct marketing;

- details of the period for which the personal data will be retained, or where it is not possible to determine the said period at the time of the giving of the information, the criteria used to determine the said period;

- details of the period for which the personal data will be retained, or where it is not possible to determine the said period at the time of the giving of the information, the criteria used to determine the said period;

- details of the recipients or categories of recipients with whom the Council shares the data;

- an explanation of the logic used in any automated decision-making;

- portability (transfer) of data when requested and where technically feasible;

- information detailing the rights of the data subject to lodge a complaint with the Data Protection Commission and the contact details of the Commission.

17. Restriction of rights of access

The right of access is restricted where the data are:

- required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders, or assessing moneys due to the State or a local authority;

- subject to legal professional privilege;

- kept only for statistical or research purposes and the results are not made available in a way that identifies data subjects;

18. Provision of access to third parties

A data subject is entitled to access only his or her own personal data. The personal information of a data subject, including confirmation of attendance or contact details, must not be disclosed to a third party, be they potential employer, professional body and so on, without the consent of the individual concerned.

19. Limitations on the use of personal data for research

The Acts require that personal data shall be kept only for one or more specified, explicit and legitimate purposes and shall not be further processed in a manner incompatible with those. This restriction may limit the usefulness of data for research purposes. If personal data are made anonymous, however, they cease to be personal data subject to the terms of the Acts.

20. Right of rectification or erasure

Data subjects have a right to have personal data rectified, or blocked from being processed, or erased where the data controller has contravened the Acts. In order to comply with the above rights of access, rectification or erasure, personal data must be held securely in a format which ensures that the personal data can be located and collated quickly and efficiently.

21. Responsibilities of data subjects

- Data subjects should be informed of how to keep their personal data up to date.

- Elected Members, staff and other data subjects are responsible for:
    - checking that any information that they provide to the Council is accurate and up to date;

- informing the Council of any changes in information that they have provided, such as changes of address;
- checking the information the Council sends out from time to time, giving details of information kept and processed;
- informing the Council of any errors or changes.

Further information

These guidelines are intended as a general introduction and are not an authoritative interpretation of the law. Extensive information is available from the Data Protection Commission's website, www.dataprotection.ie, or from the Data Protection Commission, 21 Fitzwilliam Square South, Dublin 2 D02 RD28.

If you have any questions or require clarification on any aspect of this document, please contact Brendan Hynes, Data Protection Officer, South Dublin County Council, County Hall, Tallaght, Dublin 24 D24 YNN5.