KILKENNY COUNTY COUNCIL

DATA PROTECTION COMPLIANCE GUIDELINES FOR STAFF

1. ***Purpose of Data Protection***

The Data Protection Acts 1988 to 2018 govern the processing of all personal data.

The purpose of these Acts 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 guidelines is to assist our 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.
- *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 organistation, company etc.
- *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.

4. ***Role of Data Protection Commissioner***

The Data Protection Commissioner, with whom the Council is registered as a Data Controller (Registration Number 0268/A), oversees compliance with the terms of the legislation. The Commissioner 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. This penalty is significant. A data subject now has rights to claim compensation for breaches of their 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:

(i) obtain and process the data fairly;

(ii) keep only for one or more specified and lawful purposes;

(iii) use and disclose only in ways compatible with the purposes for which it was initially given;

(iv) keep safe and secure;

(v) keep accurate, complete and up-to-date;

(vi) ensure that it is adequate, relevant and not excessive;

(vii) retain no longer than is necessary for the specified purpose or purposes;

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

6. ***Application of the Rules of Data Protection***

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

Obtaining & 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, of the categories of person/organisation to whom the data may be disclosed, of non-obligatory or optional answers in forms, of the right of access to the data and of the right of rectification of the data.

- Obtain personal data only when there is a clear purpose for so doing, obtain only whatever personal data is necessary for fulfilling that purpose and ensure data are used only for that purpose.
- The use of Council's data processing facilities (including computers) in capturing and storing personal data for non-work related purposes must not take place.

- Inform data subjects about what personal information is held by the Council, what it will be used for and to whom it may be disclosed.
- 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.

Disclosing Personal Data

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 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, do not disclose to any third party any personal data without the 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 subject to confirm facts that should be known only to them, such as date of birth, account number, etc. The date and time of the giving of verbal consent should be recorded in writing.
- Verbal consent to 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 Gardai for example, for the prevention of crime 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 only be disclosed to work colleagues where they have a legitimate interest in the data in order to fulfill administrative functions. Be satisfied of the need to disclose.
- 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.

Permitted disclosures of personal data

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

- authorised 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;
- 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 to the data subject;
- disclosed at the request or with the consent of the data subject;

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 passwords, encryption, access logs, backup, etc.
- 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 your personal computer, ensure the hard drive is cleaned by an appropriate IT staff member.
- Special care must be taken where laptops and personal computers containing personal data are used outside the Council.
- 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.

Accuracy & Completeness of Personal Data
Administrative procedures should include review and audit facilities so that personal data is accurate, complete and kept up-to-date.

Retention of Personal Data
Data should not be kept for longer than is necessary for the purpose for which it was collected. Data already collected for a specific purpose should not be subject to further processing that is not compatible with the original purpose.

Disposal of Personal Data
Personal data should be disposed of when it is no longer needed 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.

RIGHTS OF DATA SUBJECTS

Right of Access
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 thirty days:

- a copy of his or her personal data;
- the purpose of processing the data;
- the persons to whom the Council discloses the data;
- an explanation of the logic used in any automated decision-making;
- a copy of recorded opinions about him or her, unless given in confidence.

Restriction of Rights of Access
The right of access is restricted where the data is:

- required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders, or assessing moneys due to the State;
- 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;
- back-up data.

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 etc., without the consent of the individual concerned.
An agreement may be made to forward a communication to a data subject on behalf of a third party, but no information should be disclosed about the data subject.

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 is made anonymous, however, it ceases to be personal data subject to the terms of the Acts.

In addition, certain data protection rules are relaxed for personal data kept for statistical, research or other scientific purposes, so long as the data is not used in a way that may harm the data subject. The rules in question being the restrictions on further processing personal data that is incompatible with the original purpose, on not keeping data longer than necessary for the purpose and on not disclosing the purpose when the data was obtained. It should be noted that if research data is retained in personally identifiable format they may be subject to an access request from a data subject and are subject to restrictions on the transfer of data outside the European Economic Area.

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, the Council should ensure that personal data can be located and collated quickly and efficiently:

- ensure personal data is in a format that is easy to locate and collate;
- verify that the access request and the personal data released refers to the same individual;
- know exactly what data is held on individuals, and by whom;
- hold personal data in a secure central location.

Responsibilities of data subjects

- Data subjects should be informed of how to keep their personal data up to date.
- 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 (the Council cannot be held responsible for any errors unless previously informed).

FURTHER INFORMATION

These guidelines are intended as a general introduction to Data Protection and are not an authoritative interpretation of the law.

If you have any queries or require clarification on any aspect of this document, please contact Anne Maria Walsh, Data Protection Officer, Kilkenny County Council, County Hall, John Street, Kilkenny.

Extensive information is available from the Data Protection Commissioner's website, www.dataprotection.ie, or from the Office of the Data Protection Commissioner, Canal House, Station Road, Portarlington, Co. Laois.