2.4 Application of the Rules of Data Protection

In order to ensure the Institute's compliance with these rules, the following procedures must be observed by staff at all times:

RULES NOS. 1, 2 AND 6

Obtaining and processing all personal data fairly

Personal data is obtained fairly if the data subject is aware of the purpose for which DIT is collecting the data at the point of collection, 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 are necessary for fulfilling that purpose and ensure data are used only for that purpose.
- It follows that use of DIT data processing facilities in capturing and storing personal data for non-DIT purposes must not take place.
- Inform data subjects of what personal information is held by DIT, 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 that consent. Consent cannot be inferred from non-response in the case of sensitive personal data.

RULE NO. 3

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 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 data subject to confirm facts that should be known only to them, such as date of birth, student number, etc. The date and time of the giving of the 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 Gardaí 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 interest of the data subject (see below for permitted disclosures under the DP Acts).

- Personal data should only be disclosed to work colleagues where they have a legitimate interest in the data in order to fulfil administrative functions. Be satisfied of the need to disclose.

- Personal data should not be disclosed outside of the European Economic Area 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 DP Acts provide for disclosures, where data are:

- Authorised for safeguarding the security of the State (if it is in the opinion of a member of the Garda Siochana not below the rank of chief superintendent or an officer of Permanent Defence Forces holding an army rank not below that of colonel);
- Required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders, or assessing moneys due to the State, a local authority or a health board;
- Required to protect the international relations of the State;
- Required urgently to prevent injury or damage to health or serious loss of or damage to property;
- Required by law or a court order;
- Required for legal advice or legal proceedings;
- Disclosed to the data subject or to a person acting on his/her behalf;
- Disclosed at the request or with the consent of the data subject or a person acting on his/her behalf.

RULE NO. 4

Securing personal data

DIT must protect personal data from unauthorised access when in use and in storage and must be protected from inadvertent destruction, amendment, loss, disclosure, corruption or unlawful processing.

- Personal electronic data should be subject to appropriate stringent controls, such as passwords, encryption, access logs, back-ups, 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 PC, ensure the hard drive is cleaned by an appropriate IT staff member.
- Special care must be taken where laptops and PCs containing personal data are used outside the Institute.
- Health and social work personal data can only be disclosed following consultation with the relevant professional.
- The Institute, on disclosing personal data to a Data Processor, should do so only under a written contract specifying the security rules to be followed.

RULE NO. 5

Accuracy and completeness of personal data

Administrative procedures should include review and audit facilities so that personal data are accurate, complete and, where necessary, kept up-to-date. Review and audit procedures should be in place to monitor that this is being achieved.

Please refer to section below on 'Responsibilities of data subjects', and particularly the requirement that data subjects should inform DIT of errors in or changes to data. While DIT cannot be held responsible for errors unless previously informed, once informed, it is imperative that the data are amended accordingly.

RULE NO. 7

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. Personal information should only be held for periods specified in DIT's Records Retention Schedules.

Disposal of personal data

Personal data should be disposed of when they are no longer needed for the effective functioning of DIT. The method of disposal should be appropriate to the sensitivity of the data. Shredding or incineration is appropriate in the case of manual data and reformatting or overwriting in the case of electronic data. Particular care should be taken when PCs are transferred from one person to another or outside DIT or are being disposed of.

RULE NO. 8

Rights of data subjects

Right of access

The DP 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 forty days, or sixty in the case of examination data:

- A copy of his or her personal data;
- The purpose of processing the data;
- The persons to whom the Institute 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.

A maximum fee of €6.35 may be charged.

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;
- 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 his or her own personal data only. The personal information of a data subject, including confirmation of attendance at DIT or contact details, must not be disclosed to a third party, be they parent, potential employer, employer, professional body, sponsor, 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. In the case of research surveys where there is an agreement to forward documentation to data subjects, a notice should be included to the effect that no personal information has been released.

Limitations on the use of personal data for research

All researchers, be they students or staff, involved in collecting personal data, especially sensitive personal data, must comply with the requirements of the DP Acts. Initially, they must ensure that data are obtained and processed fairly. It is essential that the necessary consent from data subjects is obtained. Whenever possible, personal data should be rendered anonymous.

The DP 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 and are no longer subject to the terms of the DP Acts.

In addition, certain Data Protection rules are relaxed for personal data kept for statistical or research purposes, so long as the data are not used in a way that may harm the data subject. The rules in question are the restrictions on further processing personal data which 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 were obtained. It should be noted that if research data are retained in personally identifiable format it may be subject to an access request from a data subject and is 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 DP Acts.

In order to comply with the above rights of access, rectification or erasure, ensure that personal data can be located and collated quickly and efficiently. The following guidelines should be followed in this respect:

- Ensure personal data are in a format that is easy to locate and collate.
- Verify that the access request and the personal data released refer to the same individual.

- Know exactly what data are held on individuals, and by whom.
- Hold personal data in a secure central location.

Responsibilities of data subjects

- All staff, students and other data subjects are entitled to be informed how to keep their personal data up-to-date

- All staff, students and other data subjects are responsible for:

    - Checking that any information that they provide to DIT is accurate and up to date;
    - Informing DIT of any changes of information which they have provided, e.g. changes of address;
    - Checking the information that DIT sends out from time to time, giving details of information kept and processed;
    - Informing DIT of any errors or changes (DIT cannot be held responsible for any errors unless previously informed).