Appendix 2

Staff / Student Guidelines : Data Protection

Date last revised: October 2017

As an employee/student of DkIT and a Data Processor - How to ensure compliance with the eight rules of data protection

The Institute's Data Protection Policy sets out the arrangements in place to ensure that all personal data records held *by* the school/department/function are obtained, processed, used and retained in accordance with the following eight rules of data protection (based on the Data Protection Acts) :

1. Obtain and process information fairly
2. Keep it only for one or more specified, explicit and lawful purposes
3. Use and disclose it only in ways compatible with these purposes
4. Keep it safe and secure
5. Keep it accurate, complete and up-to-date
6. Ensure that it is adequate, relevant and not excessive
7. Retain it for no longer than is necessary for the purpose or purposes
8. Give a copy of his/her personal data to that individual on request.

The minimum age at which consent can be legitimately obtained for processing and disclosure of personal data under rules 1 and 3 above is not defined in the Data Protection Acts. However, guidance material published on the Data Protection Commissioner's website states the following:

"As a general rule in the area of education, a student aged eighteen or older may give consent themselves. A student aged from twelve up to and including seventeen should give consent themselves and, in addition, consent should also be obtained from the student's parent or guardian. In the case of students under the age of twelve consent of a parent or guardian will suffice."

The following prompt questions should be regarded as a checklist in proofing the arrangements for adherence to each of the eight rules:

1. Obtain and process information fairly: prompt questions

- Are procedures in place to ensure that staff members, parents/guardians and students are made fully aware when they provide personal information of the identity of the persons who are collecting it, the purpose in collecting the data, the persons or categories of persons to whom the data may be disclosed and any other information which is necessary so that processing may be fair
- Is personal information processed fairly in accordance with the Data Protection Acts, with consent being obtained from staff members, parents/guardians or students, where required?

- Is sensitive personal information processed fairly in accordance with the Data Protection Acts, with explicit consent being obtained from staff members, parents/guardians or students, where required?

2. Keep it only for one or more specified, explicit and lawful purposes: prompt questions

- Do the persons whose data is collected know the reason/s why it is collected and kept?

- Is the purpose for which the data is collected and kept a lawful one?

- Is school management aware of the different sets of data which are kept and the specific purpose of each?

3. Use and disclose it only in ways compatible with these purposes: prompt questions

- Is data used only in ways consistent with the purpose/s for which it was obtained?

- Is data disclosed only in ways consistent with that purpose?

- Is there a procedure in place, which is in accordance with the Data Protection Acts to facilitate the transfer of information to another college when a student transfers?

- In what circumstances will personal data be disclosed to third parties, including the Department of Education and Science, Gardaí, in legal proceedings, HSE personnel etc.?

- Is there a procedure in place, which is in accordance with the Data Protection Acts to facilitate the transfer of personal data abroad?

  Exceptions to disclosure rule:

  - Data can be disclosed when required by law
  - Data can generally be disclosed to an individual himself/herself or with his/her consent (see 8 below).

4. Keep it safe and secure: prompt questions

Appropriate security measures must be taken against unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction.

- Is access to the information (including authority to add/amend/delete records) restricted to authorised staff on a "need to know" basis?
- Who has access to what information based on this "need to know" policy?
- Are computer systems password protected?
- Is information on computer screens and manual files kept out of view of callers to the school/office?
- Are back-up procedures in operation for computer held data, including off-site back-up?
- Are all reasonable measure taken to ensure that staff are made aware of the security measures, and comply with them?
- Are all waste papers, printouts etc. disposed of carefully?
- Are steps taken to ensure that no unauthorised person can access data from computers which are no longer in use or subject to change of use?
- Is there a designated person responsible for security?
- Are there periodic reviews of the measures and practices in place?
- Are premises secure when unoccupied?
- Is there a contract in place with any data processor which imposes an equivalent security obligation on the data processor?

5. Keep it accurate, complete and up-to-date: prompt questions

- Are clerical and computer procedures adequate to ensure high levels of data accuracy?
- Are appropriate procedures in place, including periodic review and audit, to ensure that each data item is kept up-to-date?

Note: While this rule applies to all computer held data and any new manual records created from July 2003, it will only apply to existing manual records from October 2007.

6. Ensure that it is adequate, relevant and not excessive: prompt questions

- Is the information held adequate in relation to the purpose/s for which it is kept?
- Is the information held relevant in relation to the purpose/s for which it is kept?
- Is the information held not excessive in relation to the purpose/s for which it is kept?

Note: While this rule applies to all computer held data and any new manual records created from July 2003, it will only apply to existing manual records from October 2007.

7. Retain it for no longer than is necessary for the purpose or purposes: prompt questions

- Is a defined policy in place for the retention periods for all items of personal data kept?
- Are there management, clerical and computer procedures in place to implement such a policy?

Note: While this rule applies to all computer held data and any new manual records created from July 2003, it will only apply to existing manual records from October 2007.

In general, personal data should not be kept for any longer than is necessary to fulfil the function for which it was first recorded. Retention times cannot be rigidly prescribed to cover every possible situation and schools/departments/functions need to exercise their individual judgement in this regard in relation to each category of records held.

8. *Give a copy of his/her personal data to that individual on request (Data Access Request)*

On making an access request any individual about whom you keep personal data, is entitled to:

- a copy of the data which is kept about him/her
- know the purpose/s for processing his/her data
- know the identity of those to whom the data is disclosed
- know the source of the data, unless it is contrary to public interest
- know the logic involved in automated decisions
- a copy of any data held in the form of opinions, except where such opinions were given in confidence.

Scenarios

- If you have to share personal data in the course of performing your daily functions, make sure you only share the data with colleagues who **need to know** it.
- If a **parent / guardian** of a student contacts you to request their son or daughter's personal data (e.g. exam results, registration details) you should **not** release that data unless you have the written consent of the student to do so.
- If you are **emailing** more than one student at a time, you should always use the "Bcc" option to avoid sharing students' personal data (email address) with other students. Student email lists should not be shared with class reps or student societies. If a class rep wants to email all the students in their class, you could offer to forward the email on their behalf.
- If you are unsure as to whether a particular set of data should be retained or disposed of, refer to the Records Management Policy and the record retention schedule pertinent to your own area. The Data Protection Act does not specify timelines for records retention so records are retained in line with best practice and other necessary timelines as set out by Finance/EU regulations etc.
- If a **data breach** occurs in your area, you should immediately contact the Freedom of Information Officer Ms Loretto Gaughran and refer to the Personal Data Security Breach Management Procedures for further details on how to proceed.

Tips for Staff on Data Protection:

1. Become familiar with DkIT's Data Protection policies and procedures – located on DkIT Webpage.

2. Complete Data Protection training – offered on an annual basis in house.

3. Do not retain excess data, just record only what you need.

4. Keep data up-to-date and accurate.

5. Keep data safe and secure: keep offices/filing cabinets locked when not in use. Operate a clean desk policy.

6. Password-protect your computer and/or device, and never record or share your password. Use antivirus software and be aware of phishing emails! See Computer Services webpage for further advisement.

7. Back up digital files regularly.

8. Do not disclose personal data to a third party (even at the request of the data subject's family or friends) without the data subject's express consent.

9. Regularly review the data you hold and dispose of data you no longer need by confidential shredding or deletion. Don't forget your deleted items folder and recycle bin, and take appropriate steps to clear computer hard drives before disposal.

10. Take extra care with sensitive data such as medical or financial information, and only store sensitive data on computers or devices which are password-protected and have suitable encryption software installed

Please refer to other Institute documentation relating to Data Protection such as:

- DP Policy & Procedures
- Personal Data Security Breach Management Procedures
- CCTV Policy
- How to Make an Access Request
- Records Retention Schedule