Dublin City University
Data Protection Guidelines
Data Protection Guidelines

PURPOSE: To ensure that the University complies with the Data Protection Acts 1988 & 2003.

These guidelines are a summary of the key policy statements taken from the University's Data Protection Policy. The purpose of the guidelines is to make users aware of their obligations regarding the processing and confidentiality of any personal data held by the University. Personal information is defined as information which relates to a living individual who can be identified from the data. It is essential that you consult the more detailed information available in the University's Data Protection Policy.

- Anyone processing or using personal information on behalf of the University must adhere to the Data Protection Obligations relating to personal data, as detailed in the University's Data Protection Policy. These rules can be summarised as follows:
  - be processed fairly and lawfully;
  - be obtained for specified and lawful purposes and only processed in accordance with those;
  - be adequate, relevant and not excessive;
  - be accurate and where necessary up-to-date;
  - be kept for no longer than necessary;
  - be processed in accordance with Data Subjects’ Rights;
  - be kept securely;
  - not be transferred to countries without adequate protection.

- Individuals for whom personal information is being held have the responsibility to ensure its accuracy.

- Sensitive personal data should only be processed if Data Subjects have given their explicit consent.
- Personal information no longer required should be disposed of in a manner that protects the security and confidentiality of the data.

- It is University policy for encryption software to be installed on all DCU owned laptops and it is the responsibility of the staff member to ensure this software is operating correctly.

- A Data Breach, i.e. the loss of control of personal data in manual or electronic form, must be reported immediately to the university Data Protection Officer. (See DCU Data Breach – Code of Practice.)

- USB devices must not be used to store sensitive personal information.

Disclosure of personal data to third parties is allowed only where the Data Subject has given consent, or in certain other limited circumstances (see Data Protection Policy). These include:

- For research purposes (see Research and Personal Data section within Data Protection Policy);
- For the prevention or detection of crime;
- Where it is required by law;
- Where it is a statutory obligation;
- For legitimate purposes balanced against the rights and interests of the data subject.

It is also the responsibility of staff members working as supervisors of students carrying out research projects, where those students collect personal data, to take responsibility for that personal data, and to make the student aware of the Data Protection Obligations. This could be done by referring them to the Data Protection Policy.

Staff should also be aware of the DCU’s Data Breach – Code of Practice.
FOR FURTHER INFORMATION:

Within DCU, the designated Data Protection Officer has responsibility for the co-ordination of Data Protection issues and any queries and clarifications should be directed to Data Protection Officer.

More complete information is available in DCU’s Data Protection Policy or from the Office of the Data Protection Commissioner at: http://www.dataprotection.ie