



Code: QA400
Title: Data Protection Policy
Date: 09/10/2012
Approval: UMT

1. Purpose

The purpose of this policy is to advise staff of their responsibilities with regard to the handling of Personal Data as set out in law, in accordance with the Data Protection Acts 1988 and 2003 (as amended) ("the Act"). It should be noted that the Act also applies to paper records.

Personal Data must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

2. Definitions

"Personal Data" means 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.

"Sensitive Personal Data" means Personal Data as to –

- (a) racial or ethnic origin, political opinions or religious or philosophical beliefs.
- (b) membership of a trade-union.
- (c) physical or mental health or sexual life.
- (d) the commission or alleged commission of any offence, or any proceedings for an offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

"Data Processing" means creating /amending /storage/retrieval or communication of information or data.

"Data Controller" means the person who, either alone or with others, controls the contents and use of personal data and sensitive personal data. In the University, this can include each and every person who handles Personal Data.

Data Protection Principles

The University will administer its responsibilities in accordance with the eight stated data protection principles outlined in the Act as follows:

	Data Protection Principle	University Action
1.	Obtain and process information fairly.	Obtain and process Personal Data fairly and in accordance with the fulfilment of its functions.
2.	Keep data only for specified, explicit and lawful purposes.	Keep data for purposes that are specific, lawful and clearly stated. Only process in a manner compatible with these purposes.
3.	Use and disclose data only in ways compatible with these purposes.	Only disclose personal data that is necessary for the purpose/s or compatible with the purpose/s for which it collects and keeps the data.
4.	Keep data safe and secure.	Take appropriate security measures against

		unauthorised access to Personal Data. High standards of security are essential.
5.	Keep data accurate, complete and up-to-date.	Ensure procedures are adequate to ensure high levels of data accuracy. Put in place appropriate procedures to assist staff in keeping data up-to-date.
6.	Ensure that data are adequate, relevant and not excessive.	Personal data held will be adequate, relevant and not excessive.
7.	Retain data for no longer than necessary.	Develop a policy on retention periods for Personal Data.
8.	Give a copy of his/her Personal Data to an individual, on request	Procedures ensure that data subjects can exercise their rights of access.

Staff/Data Controller Responsibilities

Any staff member of NUI Galway who handles Personal Data must comply with the Data Protection Principles at 3 above. In addition, they must report any loss of Personal Data to the NUI Galway Data Protection Officer dataprotectionofficer@nuigalway.ie

Individual Rights

The individuals for whom the University stores personal data have the following rights:

- To have their personal data obtained and processed fairly, kept securely and not illegitimately disclosed to others.
- To be informed of the identity of the Data Controller and of the purpose for which the information is held.
- To get a copy of their Personal Data by requesting same from the Data Protection Officer in writing, individual will receive a copy of their data within 40 days of receipt of the request by the Data Protection Officer.
- To have their personal data corrected or deleted if inaccurate.
- To prevent their personal data from being used for certain purposes: for example, one might want to have the data blocked for research purposes where they are held for other purposes.
- Under Employment Rights, not to be forced to disclose information to a prospective employer. No one can force another person to make an access request, or reveal the results of an access request, as a condition of recruitment, employment or provision of a service. Where vetting for employment purposes is necessary, this can be facilitated where the individual gives consent to the data controller to release personal data to a third party.

It should be noted that under the Freedom of Information Act (1997 and 2003) records containing personal information may be released to a third party, where the public interest so requires.

Access Requests

Data subjects can request a copy of their personal data by submitting a request in writing to Data Protection Officer, NUI Galway, University Road, Galway. The University may seek proof of identity with regard to access requests (e.g. a copy of passport, drivers licence or other valid form of identification).

Data Security Breach

In the event of an incident which gives rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data, the matter must be brought to the attention of the Secretary of the University and the Data Protection Officer as soon as is practical. Every effort should be made to remove the risk and to ensure that the data subjects are informed.

3. Responsibilities

The University has overall responsibility for ensuring compliance with the Data Protection legislation. However, all employees of the University who collect and/or control the contents and use of personal data are also responsible for compliance. The University will provide support, assistance, advice and training to all Departments, Offices and staff.

Name	Responsibility
UMT	Policy Owner
Data Owners	Ensuring implementation of policy.
Internal Audit	Monitoring and reporting compliance with the policy
Secretary	Data Controller
Data Protection Officer	Revisions to the policy Reporting of data breaches to Data Protection Commissioner
All staff engaged in dealing with personal/sensitive personal data	Compliance with policy

4. Related Documents /Attachments

QA402 Data Classification Policy

QA401 Data Handling Policy

Student Data Usage Policy