NUI Galway
OÉ Gaillimh

Policies and Procedures

Code: QA400
Title: Data Protection Policy
Date: 27 November 2018
Approval: UMT

1. Purpose

This policy is a statement of the University's commitment to protect the rights and privacy of individuals in accordance with Irish Data Protection Acts 1988-2018 (as may be amended) ("the Act"), and the European General Data Protection Regulation 2016 ("GDPR"). The purpose of this policy is to advise staff and students and other members of the University community of their responsibilities with regard to the handling of Personal Data and Special Categories of Personal Data as set out in Irish and European Law.

2. Description

NUI Galway ("**the University**") obtains, processes, collects, keeps, uses, discloses (where permissible by law), and retains Personal Data and/or Special Categories of Personal Data (both as defined below) regarding its staff, students, service users and other individuals who come in contact with, avail of the services of or engage in business with the University. The purpose of processing Personal Data and Special Categories of Personal Data include but are not limited to fulfilling the University's functions and obligations under University Charter, the Universities Act 1997, University Statutes and Regulations, University policies and procedures, the provision of educational courses and support services to students and staff, assessment of student engagement, the organisation and administration of courses, undertaking of research activities, the recruitment and employment of staff, compliance with statutory obligations, reporting to Government and regulatory bodies, the provision of commercial activities, the management of financial affairs, the provision of information solutions and services, the provision of library services, advertising and promoting the University, publishing University and alumni publications, and undertaking fundraising by or on behalf of the University. The University also processes personal information through CCTV systems that monitor and collect visual images for the purposes of research, security and the prevention and detection of crime and offences.

The University acknowledges that the processing of Personal Data and Special Categories of Personal Data must meet the requirements of applicable Irish and European data protection legislation. Data Protection is the safeguarding of the privacy rights of individuals in relation to the processing of Personal and Special Categories of Personal Data. The Act and the GDPR confer rights on individuals as well as responsibilities on persons and organisations processing personal data. Data protection is also an important part of the University's overall information security practices. All Personal Data and Special Categories of Personal Data must be handled safely and securely according to agreed University policy. It is required that staff and any person processing Personal Data or Special Categories of Personal Data on behalf of the University process such data in accordance with University policy and applicable law.

3. Scope:

This policy applies to:

- any person employed or engaged by the University who processes Personal Data or Special Categories of Personal Data in the course of their employment or engagement for academic, administrative, research and/or any other purpose;
- any person(including but not limited to research placements, secondments, work placements, visitors or interns) who is given access to University systems containing Personal Data or Special Categories of

Personal Data, and who processes Personal Data or Special Categories of Personal Data in the course of their access;

- any student of the University who process Personal Data or Special Categories of Personal Data in the course of their studies for academic, administrative, research and/or any other purpose;
- individuals who are not directly employed by the University, but who are employed by contractors (or subcontractors) and who process Personal Data or Special Categories of Personal Data in the course of their duties for the University;
- All locations from which University Personal Data or Special Categories of Personal Data are accessed, including access while travelling and home use;
- Any Personal Data or Special Categories of Personal Data held or transmitted in paper, physical or electronic formats and communicated verbally in conversation or over the telephone;
- The University's clubs and societies.

Hereinafter these are collectively referred to as "**Member**" or **"Members"**.

4. Definitions

Definitions in this policy are intended for use within the NUI Galway Policy and operational framework. They are not necessarily the same as definitions of the same terms contained in external documents, whether or not referred to in this policy. In this Policy:

"Data Controller" means— (a) a competent authority that, whether alone or jointly with others, determines the purposes and means of the processing of Personal Data, or (b) where the purposes and means of the processing of Personal Data are determined by the law of the European Union or otherwise by the law of the State, a controller nominated— (i) by that law, or (ii) in accordance with criteria specified in that law;

"Data Processor" means an individual who, or a legal person, public authority, agency or other body that, processes Personal Data on behalf of a controller, but does not include an employee of a controller who processes such data in the course of his or her employment.

"Data Subject" means a living person who is the subject of Personal Data;

"Personal Data" means information relating to— (a) an identified living individual, or (b) a living individual who can be identified from the data, directly or indirectly, in particular by reference to— (i) an identifier such as a name, an identification number, location data or an online identifier, or (ii) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual;

In practice, any data about a living person who can be identified from the data available (or potentially available) will count as personal data. This will include reversibly anonymized **("pseudonymised")** data. Where a pseudonym is used, it is often possible to identify the data subject by analyzing the underlying or related data.

"**Special Categories of Personal Data**", other than in Part 5 of the Irish Data Protection Act 2018, means— (a) personal data revealing— (i) the racial or ethnic origin of the data subject (ii) the political opinions or the religious or philosophical beliefs of the data subject, or (iii) whether the data subject is a member of a trade union (b) genetic data (c) biometric data for the purposes of uniquely identifying an individual (d) data concerning health, or (e) personal data concerning an individual's sex life or sexual orientation;

"Processing", of or in relation to Personal Data, means an operation or a set of operations that is performed on Personal Data or on sets of Personal Data, whether or not by automated means,

including— (a) the collection, recording, organisation, structuring or storing of the data, (b) the adaptation or alteration of the data, (c) the retrieval, consultation or use of the data, (d) the disclosure of the data by their transmission, dissemination or otherwise making the data available, (e) the alignment or combination of the data, or (f) the restriction, erasure or destruction of the data;

"Profiling" means any form of automated processing of Personal Data consisting of the use of the data to evaluate certain personal aspects relating to an individual, including to analyse or predict aspects concerning the individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

"Pseudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified natural person. The Data Protection Acts still apply to Personal Dara which has been pseudonymised.

5. University Member obligations

Any Member of NUI Galway who handles Personal Data or Special Categories of Personal Data must comply with the Data Protection Principles and this Policy. Compliance with this Policy and applicable law is the responsibility of all members of the University. Failure of an individual University Member to comply with this Policy may lead to action, being taken in accordance with the applicable University's procedures. Failure of a third-party contractor/subcontractor to comply with this policy may lead to termination of the contract and/or legal action. University Members embarking on new activities involving the use of Personal Data and/or Special Categories of Personal Data and that is not covered by one of the existing records of processing activities should inform the Data Protection Officer (dataprotection@nuigalway.ie) before starting the new activity.

6. University and University Member obligations regarding the Data Protection Principles

The University adheres to the principles of both the current Act and the European General Data Protection Regulation in its processing of Personal Data and Special Categories of Personal Data. In accordance with these principles, Personal Data and Special Categories of Personal Data shall be:

(a) Processed lawfully and fairly **("lawfulness, fairness and transparency")**;
(b) Collected for one or more specified, explicit and legitimate purposes and shall not be processed in a manner that is incompatible with such purposes **("purpose limitation")**;
(c) Adequate, relevant and not excessive in relation to the purposes for which they are processed **("data minimisation")**;
(d) Accurate, and, where necessary, kept up to date, and every reasonable step shall be taken to ensure that inaccurate data, having regard to the purposes for which they are processed, be erased or rectified without delay **("accuracy")**;
(e) Kept in a form that permits the identification of a data subject for no longer than is necessary for the purposes for which the data are processed **("storage limitation")**;
(f) Processed in a manner that ensures appropriate security of the data, including, by the implementation of appropriate technical or organisational measures, protection against **("integrity and confidentiality")**—
    (i) Unauthorised or unlawful processing, and
    (ii) Accidental loss, destruction or damage.

Data Subjects have a number of additional rights under the GDPR which the University will adhere to. The availability of the additional GDPR rights largely depends on the legal justification for processing by the University and there are exceptions to each of these rights. The additional rights are as follows:

- **Right of Access by the Data Subject** - Individuals have a right to request a copy of their personal

Data the University are processing about them and to exercise that right easily and at reasonable intervals.

- **Right to Object** – Data Subjects have the right to object to specific types of processing such as automated decision making and profiling.

- **Right to be forgotten (erasure)** – Data Subjects have the right to have their data erased in certain situations, such as where the data are no longer required for the purpose for which they were collected, the individual withdraws consent or the information is being processed unlawfully. There is an exemption to this right for scientific, historical or statistical research purposes if the erasure would render impossible or seriously impair the achievement of the objectives of the research. Data Subjects can ask the controller to 'restrict' processing of the data whilst complaints (for example, about accuracy) are resolved or the processing is unlawful.

- **Rights in relation to automated decision making and profiling** – The right relates to automated decisions or profiling that could result in significant affects to the Data Subject.

- **Right to Rectification** - The right to require a Controller to rectify inaccuracies in Personal Data or Special Categories of Personal Data held about them.

- **Right to Portability** – the Data Subject has the right to request their personal data in a structured, commonly used and machine-readable form so it can be sent to another Controller. This only applies to Personal Data or Special Categories of Personal Data that is processed by automated means (not paper records).

It should be noted that under the Freedom of Information Act 2014(as may be amended) records containing personal information may be released to a third party, where the public interest so requires.

The following obligations also apply:

- The University acknowledges that for some projects a Data Protection Impact Assessment (DPIA) shall be carried out. The types of circumstances in which this is required include: those involving processing of large amounts of personal data, where there is automatic processing/profiling, processing of special categories of personal data, or monitoring of publicly assessable areas (i.e. CCTV). The DPIA is a mechanism for identifying and examining the impact of new initiatives and putting in place measures to minimise or reduce risks. The advice of the Data Protection Officer should be sought where applicable
- The University shall keep a record of its data processing activities as a summary of the processing and sharing of personal information and the retention and security measures that are in place.
- The University shall provide data subjects with a 'privacy notice' or notices where appropriate to let individuals know what the University does with their Personal Data. Privacy notices are published on the University website and are therefore available to staff and students and service users from their first point of contact with the University.
- The University and all University Members who use Personal Data or Special Categories of Personal Data shall ensure that all data they hold is kept securely.
- The University and all University Members shall ensure that Personal Data or Special Categories of Personal Data is not disclosed to any unauthorised third party in any form either accidentally or otherwise.
- The University and all University Members shall ensure that University data security will be undertaken in line with ISS policies and procedures available on the University website.
- The University and all University Members acknowledge that Personal Data or Special Categories of Personal Data can only be transferred out of the European Union under certain circumstances and

the advice of the Data Protection Office should be sought.

- Individual Units within the University are responsible and accountable and shall keep records of the Personal Data and Special Categories of Personal Data that they hold.
- Individual Units within the University are responsible for ensuring the appropriate retention periods for the information they hold and manage, based on University guidance in the University Record Retention Policy. Retention periods are set based on legal and regulatory requirements, sector and good practice guidance. As a general rule, Personal Data must only be kept for the length of time necessary to perform the processing for which it was collected. Once information is no longer needed is should be disposed of securely. Paper records should be shredded or disposed of in confidential waste and electronic records should be permanently deleted.
- University Members shall consider the impact on data privacy during all processing activities.
- University Members shall consider privacy issues when considering new processing activities or setting up new procedures or systems that involve personal data.
- The University acknowledges that GDPR imposes a specific 'privacy by design' requirement emphasising the need to implement appropriate technical and organisational measures during the design stages of a process and throughout the lifecycle of the relevant data processing to ensure that privacy and protection of data is not an after-thought. The advice of the Data Protection Officer should be sought where applicable.
- The University also acknowledges that GPDR imposes a specific 'privacy by default' requirement meaning that once a product or service has been released to the public, the strictest privacy settings should apply by default, without any manual input from the end user. In addition, any personal data provided by the user to enable a product's optimal use should only be kept for the amount of time necessary to provide the product or service. If more information that necessary to provide the service is disclosed, then "privacy by default" has been breached.
- The University shall also comply with the ePrivacy Regulations 2011 (S.I. 336 of 2011) (as may be amended).

7. Right to use Personal Data

In order for it to be legal and appropriate for the University to process Personal Data at least one of the following conditions must be met:

a) The data subject has given his or her **consent**
b) The processing is required due to a **contract**
c) It is necessary due to a **legal obligation**
d) It is necessary to protect someone's **vital interests** (i.e. life or death situation)
e) It is necessary for the performance of a **task** carried out in the **public** interest or in the exercise of official authority vested in the controller
f) It is necessary for the **legitimate interests** of the controller or a third party and does not interfere with the rights and freedoms of the data subject (this condition cannot be used by public Authorities in performance of their public tasks)

Universities are classified as public authorities and therefore the use of the 'legitimate interests' justification is not possible in terms of the University's core activities (public tasks). It may be possible to use legitimate interests for processing that is undertaken outside of the University's public tasks.

In cases where the University relies on **consent** as a condition for processing personal data, it must:

- Obtain the data subject's specific, informed and freely given consent;
- Ensure that the data subject gives consent by a statement or a clear affirmative action;
- Document that statement/affirmative action;
- Allow data subjects to withdraw their consent at any time without detriment to their interests.

All processing of personal data carried out by the University must meet one or more of the conditions above. In addition, the processing of Special Categories of Personal Data requires extra, more stringent conditions to be met in accordance with Article 9 of the GDPR: https://gdpr-info.eu/art-9-gdpr/ and Sections 45-55 of the Irish Data Protection Act 2018.

8. Access Requests

Please follow the University Access Request Procedure available on the University Data Protection website. In summary, the individuals for whom the University stores Personal Data can get a copy of their Personal Data by requesting same from the Data Protection Officer in writing. The individual will receive a copy of their data within 30 days of receipt of the request by the Data Protection Officer unless extended under the Act.

9. Data Security Breach

The University Data Breach procedure is available on the University Data Protection website. In summary, 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 both the Secretary of the University and the Data Protection Officer as soon as possible.

10. Review of Policy

This Policy will be reviewed regularly in light of any legislative or other relevant developments.

11. Responsibilities

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

The following roles and responsibilities apply in relation to this Policy:

Name/Title	Roles and Responsibility
University Management Team (UMT)	Policy Owner; each member of UMT is responsible for ensuring compliance with the Data Protection Acts and this policy in their respective areas of responsibility; Responsible for reviewing and approving this Policy as recommended by the Secretary or the Data Protection Officer.
Data Owners	Ensuring implementation of policy.
Internal Audit	Monitoring and reporting compliance with the policy
Secretary	Data Controller ensuring that this Policy is reviewed and approved by the UMT as appropriate; ensuring that appropriate policies and procedures are in place to support this Policy; liaising with the UMT as appropriate; ensuring that any data security breaches are properly dealt with.

Data Protection Officer	• Revisions to the policy; • Act as a contact point for and cooperating/liaising with the Data Protection Commissioner where necessary or appropriate, including in the event of a data security breach; • Advise where necessary the Controller in relation to Data Protection Impact Assessments; • Have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing; • Inform and advise the University and University Members of the obligations under this Policy, the Act and GDPR; • Monitor the Universities compliance with GDPR and this Policy; • Reporting of data breaches to Data Protection Commissioner; • Involved properly and in a timely manner in all issues relating to the protection of personal data; • Maintain a record of all personal data security breaches; • Process formal Data Access Requests; • Respond to Data Access Requests; • Liaise with relevant staff in the University departments/offices regarding Data Access Requests; • Initiate regular reviews of data protection policies and procedures and ensure documentation is updated as appropriate; • Organise targeted training and briefing sessions for University staff as required; • Provide advice and guidance to University staff on data protection matters.

Heads of School/Unit	• ensuring compliance with the Data Protection Acts and this policy in their respective areas of responsibility; • nominating a suitable member of staff to be responsible for coordinating Data Protection compliance matters within each of the areas under their remit; • enabling the Data Protection Officer to maintain a record of processing activities by compiling, approving and returning the information required for the compilation of a register of Personal Data and Special Categories of Personal Data to the Data Protection Officer; • Drawing the attention of the staff to the requirements of the policy; • Ensuring that staff who have responsibility for handling personal data are provided with adequate training; • Ensuring that job descriptions for members of staff or agreements with third parties reference data privacy responsibilities; • Data sharing is conducted in accordance with University guidance
All Staff or Students or Members engaged in dealing with personal or Special Categories of Personal Data	• Acquaint themselves with, and abide by, the rules of Data Protection set out in this Policy; • Understand what is meant by 'personal data' and 'special categories of personal data' and know how to handle such data; • Keep personal data up-to-date; • Contact the Data Protection Officer if in any doubt; • Must complete relevant training and awareness activities provided by the University to support compliance with this policy; • Should take all necessary steps to ensure that no breaches of information security result from their actions; • Use a minimum of personal data and only hold it for as long as is strictly necessary; • Must report all suspected and actual data security breaches to their head of school/function who must in turn report the incident immediately to the Data Protection Officer; • Must inform the University of any changes to the information that they have provided to the University in connection with their employment or studies (e.g. changes of address or bank account details); • Not jeopardise individuals' rights or risk a contravention of the Act.

12. Related Documents /Attachments

QA402 Data Classification Policy
QA401 Data Handling Policy
QA442 Record Retention Policy
Data Access Request Procedure
Data Breach Procedure

In addition, the following legislation must be considered in conjunction with this policy:

- Electronic Privacy Regulations 2011 (SI 336/2011) (as may be amended)

13. Further Information

If you have any queries in relation to this policy, please contact:

The Data Protection Officer
NUI Galway, Room A129
The Quadrangle
NUI Galway
University Road
Galway
Email: dataprotection@nuigalway.ie
Tel: (091) 492150

14. Disclaimer

The University reserves the right to amend or revoke this policy at any time without notice and in any manner in which the University sees fit at the absolute discretion of the University or the President of the University.