OLLSCOIL NA GAILLIMHE
UNIVERSITY OF GALWAY

Policies and Procedures

Code:	**QA401**
Title:	**Data Handling Policy**
Date:	**25 November 2022**
Approval:	**IT Security and Data Protection Committee**

1.0 Purpose

Protection of sensitive data held in the University and being handled by university staff as authorised users. It will also ensure the University remains compliant with the requirements of the Data Protection Acts 1988-2018 (as may be amended) and the European General Data Protection Regulations 2016 (“GDPR”).

2.0 Description

2.1. Definitions /Terms

Data Owner –means Head of School or Unit Head or Principal Investigator for Research Project who is responsible for classifying under his/her control data and generating guidelines for its lifecycle management. These are usually the officers responsible for the initial collection/input and use of the data. Synonymous with “information owner.”

Authorised User– Individual who has been given access to the data based on Data Owners consent or agreed the individual meeting agreed criteria for access as set down by the Data Owner.

Personal Data – 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, psychological, genetic, mental economic, cultural or social identity of the individual.

Special Categories of Personal Data – other than in Part 5 of the 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.

2.2 Data Handling

The table at Schedule 1 describes the data handling policy which shall be applied based on the data classification policy QA402.

3.0 Responsibilities

3 Responsibilities of University Units and Employees

3.1 The University operates a hierarchical system of management whereby responsibility for many of its functions and operations are devolved from Údarás na hOllscoile (Governing Authority) to the University Management Team and ultimately to heads of academic, research, project principal investigators and administrative support units.

3.2 Operational responsibility for the implementation of this Policy rests with the Data Owners including but not limited to the heads of each academic/research/administrative area and support units.

3.3 Various University employees are in possession and control of documentation and records relevant to their functions and as such are considered 'Data Owners' of same. Data Owners are responsible for the management and retention and disposal of such documentation and records. Examples of documentation and record 'Data Owners' include: -

Data Owner:	**Documentation and Records:**
Buildings Office	Property Title and other Deeds
Library	Library Records
Human Resources Office	Employment Records
Financial Accounting Office	Payroll, Non-Pay and Income Records
Procurement & Contracts Office	Centralised Tender Application and Awards
Health & Safety Office	H & S Records
Research Accounting Office	Scholarships and Research Cost Statements
Office of Vice-President for Research	Research Applications, Funder Contracts, Patent & IP Records
Head of Corp & Legal Affairs	Legal Records
Academic Secretary	Academic and Governance Records
ISS	Centralised IT and Electronic Records
Principal Investigators	Project records

3.4 Where records are used by more than one department/office/unit, clarity about which office has primary/final responsibility for management of the records should be established between the relevant offices.

3.5 The confidentiality of information within records must be safeguarded at all times. It is the responsibility of each department/office/unit to ensure that the appropriate security measures are observed for maintaining records containing personal or other confidential information.

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

Name	**Responsibility**
Chief Operating Officer	Policy Owner
Data Owners	Implementation of policy by authorised users.
Authorised Users	Implementation of the policy.
Internal Audit	Monitoring and reporting compliance with the policy
Data Protection Officer	Revisions to the policy

4.0 Attachments/Related Policies

QA400 Data Protection Policy
QA402 Data Classification Policy

Table: QA401 Data Handling Policy

Classification➔ **Activity 🡻**	**University of Galway Highly Restricted**	**University of Galway Restricted**	**University of Galway Controlled**
Access Control	Available only to those who have an absolute requirement for access. This requirement should be submitted in writing and authorized by the Data Owner. Access should be reviewed on a regular basis. Where access is granted to a third party, a non- disclosure agreement should be in place.	Available to authorized users only. Access should be reviewed on a regular basis. Where access is granted to a third party, a non-disclosure agreement should be in place.	Available to all University of Galway staff and others (providing that there is a form of confidentiality ensured) as required.
Backup	Data should be highly protected. Backups should be taken on a nightly basis, subject to data change rate. Backups should be held in a secure fire-proof-location removed from the data source. This data is a candidate for online mirroring to a remote location.	Data should be protected by backups and held in a secure location away from the source data.	Data should be protected by backup
Labelling	Follow process in place which must be documented by each Data Owner.	Irrespective of the data classification labels should be used to convey the importance of the data where appropriate.	Irrespective of the data classification labels should be used to convey the importance of the data where appropriate.
Physical Transfer (paper)	Follow process in place which must be documented by each Data Owner. Such process could include for example that documents be counted and distributed immediately prior to the agenda item at the meeting; and watermarked with each individual’s name; and collected immediately following the agenda item and counted again to ensure that all copies have been returned.	For all classifications of data due care should be taken in respect of the transfer of information in physical form.	For all classifications of data due care should be taken in respect of the transfer of information in physical form.

Electronic Storage	Must be stored in systems accessible only to those covered under access above. Servers which hold this data must be housed in a secure data centre environment. Storage of this data outside of the source **University of Galway** system, for example on a laptop or portable device ; must be approved in writing by the Data Owner. **Where data is held outside the source University of Galway system it must be encrypted and secured**. Where data is stored on a cloud based supplier other than those contracted by ISS , It is the responsibility of the staff member to verify that the data is stored in line with this policy and the Data Protection Policy.	Must be stored in systems accessible only to those covered under access above. **Where data is held outside the source system it must be encrypted and secured.** Where data is stored on a cloud based supplier other than those contracted by ISS, It is the responsibility of the staff member to verify that the data is stored in line with this policy and the Data Protection Policy.	Must be stored in systems accessible to those covered under access above.
Electronic Transfer – Internal to University of Galway	Data transfers shall be encrypted via an approved system and secured.	Data transfers shall be encrypted via an approved system such as HEA FileSender. Transmission	Encryption should be considered where appropriate.
Transfer – External to University of Galway	Data transfers shall be encrypted via an approved system. Shall not be emailed unless encrypted and secured.	Data transfers should be encrypted via an approved system such as HEA	Encryption should be considered where appropriate.
Disposal	Physical copies of data should be shredded. Storage media, including hard drives which have ever held such data should be disposed of in a secure manner. Please consult ISS for further information.	Physical copies of data should be shredded. Storage media, including hard drives which have ever held such data should be disposed of in a secure manner. Please consult ISS	Systems handling data may be disposed of in a normal fashion.
System Controls	Information may only be processed on approved University of Galway systems, which are managed by a designated systems manager.	Information may only be processed on approved University of Galway systems, which are	Information should be processed on the basis of basic best practice.
System Availability	Where the data availability requirement is high, consideration should be given to hosting this data on a resilient infrastructure that would protect against outages.	Information should be subject to the appropriate industry standards that ensure the availability of the information when and where	Information should be subject to the appropriate industry standards that ensure the availability of