Ollscoil na Gaillimhe
University of Galway

Polasaí agus Nósanna Imeachta/Policies and Procedures

Code	**QA445**
Title	**Staff Data Usage Policy**
Policy Owner	**Chief Operating Officer**
Date	**3 September 2025**
Approved By	**IT Security and Data Protection Committee**

1. Introduction

This notice explains how University of Galway as a Data Controller collects, uses and shares personal data relating to prospective, current and former employees, job applicants, self-employed contractors and consultants, and voluntary workers (an "employee"). All Personal Data collected by University of Galway will be treated in accordance with the University of Galway Data Protection Policy and applicable Irish and European legislation.

2. What is Personal Data?

Personal data is any information relating to a living individual which allows either directly or indirectly the identification of that individual. Personal Data can include a name, an identification number, details about an individual's location or any other detail(s) that is specific to that individual and that would allow the individual to be identified or identifiable.

Employee personal data may include "special categories of data" described under the GDPR. Special categories data include information on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

3. How we collect your Personal Data

University of Galway collects personal data from an employee primarily during the application, recruitment and appointment process, supplemented by information generated in the course of employment. Personal Data collected will be used by University of Galway only in accordance with the purposes outlined in this notice.

Employee(s) may provide University of Galway with personal data about other individuals, for example emergency contact details and information about employee family circumstances and dependents. Employee(s) should notify the relevant person that they are providing their contact details to University of Galway as employee listed emergency contact.

4. Types of Personal data collected by University of Galway

University of Galway collects all types of personal data including but not limited to:

- Contact information, email addresses, telephone numbers
- HR files and records (including contracts, training records, disciplinary and grievance records, salary details, benefits, compensation type, awards, pay frequency, effective date of current compensation).
- Working time records (including annual leave and other absence records, leave status, hours worked and department standard hours), pay data, national insurance or other number, marital/civil partnership status, domestic partners and dependents).
- Information requested from external sources to assist in the consideration of promotion.
- Confirmation of fitness for work from nominated Occupational Health Providers.
- Validation of qualifications from awarding institutions.
- Taxation information from Revenue.
- Information regarding related payroll contributions or benefits from the Department of Social Welfare (including tax and insurability classification).
- CVs, cover letters and job applications (and associated purposes such as references from former employers, colleagues or other relevant parties etc), interview notes and feedback; details on performance management ratings, development programs planned and attended, e-learning programs, performance and development reviews, willingness to relocate or driver's license information.
- Data related to pensions.
- Photographs of employees and Staff Cards.
- Medical information (including medical certificates and sick notes).
- Data in relation to memberships of clubs or societies associated with University of Galway.
- Data Processed in relation to optional staff schemes or benefits.
- CCTV Footage/ANPR/Body Cams (see University of Galway CCTV procedure for further details).
- Car registration details.
- Bank account details – sort code, account number and IBAN.
- Emergency contacts.
- Dependant data.
- Awards received & professional membership information.
- Data relating to publications, invitations and other University's communications.
- E-mail addresses and phone numbers.
- Marital status.
- Gender.
- Nationality.
- Garda vetting data.
- Hosting or secondment agreements.
- Data required for the processing and progression of University Policies and Procedures.
- Data pertaining to Health and Safety issues.
- Passports.
- Visa and work permit details.
- Driving licences.
- Unsolicited job applications are often received by the University of Galway either directly or via recruitment partners. There is no obligation on University of Galway to retain or reply to unsolicited applications made and, in most cases, University of Galway will not reply to or retain an unsolicited job application.
- Access logs of university IT
- Swipe access logs of university campus

5. Purpose for which University of Galway uses employee personal data

Employee personal data will be used for various legal and practical purposes, without which University of Galway would be unable to employ its employees or recruit prospective employees. It enables University of Galway to maintain a full staff record and manage the entire employee lifecycle. Holding employee personal data enables University of Galway to meet various statutory obligations over the course of the employment and to manage relevant payments associated with an employee(s) employment.

University of Galway will routinely publish some sources of information about University of Galway that include personal data. These may include staff work telephone / email directory, graduation programmes and audio-visual representations of graduation ceremonies, prospectuses, annual reports, newsletters and staff profiles on the University website.

Depending on the employee role, University of Galway may process employee personal data for the following purposes:

- managing human resources processes such as recruitment and selection, payment of wages/salaries, statutory and other deductions, pension scheme membership, performance management, training and development.
- providing facilities such as car parking, IT services, library services, cycle-to-work scheme.
- to manage insurance/personal accident claims.
- monitoring equal opportunities and to comply with other statutory reporting requirements.
- to produce statutory and University of Galway reports using summarised statistics.
- to ensure that the digital services provided by the University of Galway are performant, reliable, secure and to support appropriate ISS incident resolution.
- disciplinary matters, staff disputes, employment tribunals.
- providing communications about University of Galway news and events.
- maintaining contact with past employees.
- provision of wellbeing and support services.
- to promote and protect equality and human rights.
- to meet health and safety obligations.
- notifying staff of opportunities open to staff.
- to ensure the safety of all staff and to facilitate mass communications in emergency situations
- to provide added protections for anyone lone working on campus.
- to ensure the prompt and effective dissemination of critical information

6. Staff Monitoring

University of Galway provides e-mail facilities and access to the internet in line with the policies and procedures of the University of Galway Information Solutions and Services unit. These policies and procedures are there to protect against the risks associated with e-mail and internet use. They include a right to monitor e-mail and web usage. Please refer to of University of Galway Information Solutions and Services policies for further details.

CCTV cameras are in operation at a range of points across the University campus, ANPR automatic number plate recognition cameras are in operation on the campus and body worn cams are used by security. The primary purpose of having CCTV and ambient recording is for security and health & safety purposes. As an ancillary use, staff monitoring will only take place in the event of an incident that requires investigation. Access to the recorded material is strictly limited to authorised personnel.

Staff can be supplied with a security access card which allows them access to buildings and/or other secured areas depending on access requirements. The primary use of such systems is for security and access. Access to access records is strictly limited to authorised personnel.

7. The legal basis for collecting personal data

Under GDPR University of Galway must have a lawful basis for collecting employee data. Please see the legal basis allowable under the GDPR: https://gdpr-info.eu/art-6-gdpr/. Any personal data provided to University of Galway on recruitment/appointment and during the course of employee employment will be processed fairly and lawfully.

The legal basis for processing employee personal data by University of Galway are:

- to fulfil the terms of an employee contract with the University of Galway;
- to comply with University of Galway legal obligations e.g. employment and equality laws and statutory deductions;
- to perform any of its public tasks as a University and Public body eg to achieve any of the objects and functions of the University under the Universities Act 1997;
- where necessary for University of Galway legitimate interests e.g. evaluating a job applicant for a role; provision of ambient CCTV on campus for health and safety reasons;
- to protect employee vital interests or those of another person e.g. where University of Galway knows or have reason to believe that an employee may suffer harm or is aware of a critical incident affecting employees.

Where special categories of data are processed by the University, the university will ensure that one of the conditions of article 9 of the GDPR is met. Please see the legal conditions allowable under the GDPR: https://gdpr-info.eu/art-9-gdpr/

8. Details of third parties with whom University of Galway share personal data

University of Galway will share employee data with the following third parties where necessary for purposes of the processing outlined above:

- Revenue
- Department of Public Expenditure and Reform
- Department of Social welfare
- Higher Education Authority (HEA)
- Department of Education and Skills
- Department of Finance
- Other Governmental Departments (as may be required within grant or other applications)
- Research sponsors/external funding agencies
- Potential employers (where employee have requested University of Galway to provide a reference)
- Occupational Health Providers and medical practitioners as specified in the sick leave policy
- Insurance brokers and providers
- Pension administrators
- External auditors
- Software vendors where necessary to provide technical support and software upgrades
- Contractors performing a service on behalf of the university under an obligation of confidentiality
- Safezone an app designed to ensure keeping safe while at university.

Where University of Galway uses third parties to process personal data on University of Galway's behalf (acting as data processors), a written contract will be put in place to ensure that any personal data shared will be held in

accordance with the requirements of data protection law and that such data processors have appropriate security measures in place in relation to employee personal data.

9. Data Transfers outside the EEA

In the course of processing employee personal data, it may be transferred outside of the European Economic Area on the understanding that University of Galway rely on legally approved mechanisms to lawfully transfer data across borders, including the Standard Contractual Clauses approved by the European Commission. For example, data may be shared during reporting on University of Galway rankings or during various applications for grants, research proposals etc.

10. How long University of Galway will keep employee data

In keeping with the data protection principles University of Galway will only store employee data for as long as is necessary. For the purposes described here University of Galway will store employee data in accordance with the University of Galway's QA442 Record Retention Policy and Schedule.

11. Employee rights

An employee has various rights under data protection law, subject to certain exemptions, in connection with University of Galway's processing of employee personal data, including the right:

- to find out if University of Galway use employee personal data, access employee personal data and receive copies of employee personal data.
- to have inaccurate/incomplete information corrected and updated.
- in certain circumstances, to have employee details deleted from systems that University of Galway use to process employee personal data or have the use of employee personal data restricted in certain ways.
- to object to certain processing of employee data by University of Galway.
- to exercise employee right to data portability where applicable (i.e. obtain a copy of employee personal data in a commonly used electronic form.
- where University of Galway have relied upon consent as a lawful basis for processing, to withdraw employee consent to the processing at any time.
- to not be subject to solely automated decision making.

12. Data Security and Data Breach

University of Galway have technical and organisational measures in place to protect Personal Data from unlawful or unauthorised destruction, loss, change, disclosure, acquisition or access. Personal Data are held securely using a range of security measures including, as appropriate, physical measures such as locked filing cabinets, IT measures such as encryption, and restricted access through approvals and passwords. For more information on security measures see the University of Galway ISS Security pages on the University of Galway website.

Particular safeguards will be put in place for the collection and processing of special categories of data and criminal convictions.

Please consult the University of Galway QA443 Data Breach Procedure respect of how a data breach is handled.

Employees of University of Galway are required to maintain the confidentiality of any data to which they have access, including all data relating to fellow staff, students, customers, clients, service providers as well as website users, members, moderators and administrators.

13. Questions or Complaints

If employee have any queries in relation to the employee personal data processed by the University of Galway, contact the Department of Human Resources in the first instance. Under Data Protection legislation, an employee is entitled to access his/her HR file directly through HR.

If employee have any queries or complaints in connection with University of Galway's processing of employee personal data, an employee can contact University of Galway's Data Protection Officer at:

The Data Protection Officer
Room A129
The Quadrangle
University of Galway
University Road
Galway
Email: dataprotection@universityofgalway.ie

.

Employees also have the right to lodge a complaint with the Data Protection Commission if an employee is unhappy with University of Galway's processing of employee personal data. Details of how to lodge a complaint can be found on the Data Protection Commission's website, or by telephoning 1890 252 231.

14. Review

This Notice will be reviewed and updated from time to time to take into account changes in the law and the experience of the Notice in practice. Any and all changes will be advised. This Notice does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this Notice will be taken seriously and may result in the invoking of appropriate disciplinary procedures.

15. Responsibilities

Name (Office or position)	**Responsibility**
ICT Security and Data Protection Committee	Policy approver.
University Management Team (UMT)	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 COO or the Data Protection Officer.
Internal Audit	Monitoring and reporting compliance with the Policy
Chief Operating Officer	Policy Owner. Ensuring that appropriate policies and procedures are in place to support this Policy. Liaising with the UMT as appropriate.
Data Protection Officer	Ensuring that this Policy is reviewed and approved by the ICT Security

	Committee as appropriate: Revisions to the Policy. Act as a contact point and support for and liaising with the Unit Heads. Organize targeted Policy training and briefing sessions for University staff as required.
Heads of School/Unit	Ensuring compliance with this Policy in their respective areas of responsibility; Ensuring that staff who have responsibility for handling personal data attend Data Protection training; Ensuring Personal 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 this Policy and related policies and procedures. Understand what is meant by 'personal data' and 'special categories of personal data' and know how to handle such data. Keep staff personal data up-to-date. 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.

16. Related Documentation

- QA400 Data Protection Policy
- QA401 Data Handling Policy
- QA402 Data Classification Policy
- QA412 Student Data Usage Policy
- QA442 Record Retention Policy & Schedule
- QA443 Personal Data Breach Procedure
- QA444 Data Subject Rights 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).

17 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.