UNIVERSITY of LIMERICK
OLLSCOIL LUIMNIGH

Staff Data Protection Privacy Notice

Effective 25 May 2018

Introduction

This Privacy Notice has been developed to ensure staff feel confident about the privacy and security of Personal Data and to meet the University's obligations under the Data Protection Acts 1988 to 2018 and the General Data Protection Regulation (the "Legislation"). Those obligations, set out below, apply to employment applicants, current staff, retired staff, agency workers and contractors of the University. Under the Legislation, Personal Data is information that identifies you as an individual or is capable of doing so ("Personal Data").

To the extent the University is a 'data controller', it must comply with the data protection principles set down in the Legislation (and referenced in detail below). This Notice applies to all Personal Data collected, processed and stored by the University in the course of its activities. The purpose of this Notice is to set out the procedures that are to be followed when dealing with Personal Data and to outline how the University will collect and manage personal information in accordance with all relevant legislation and standards. The procedures set out herein must be followed at all times by the University, its employees, staff, agents, contractors, or other parties working on the University's behalf.

This Notice extends to all Personal Data whether stored in electronic or paper format.

What Personal Information does the University hold on its Staff?

The University only holds Personal Data that is directly relevant to its dealings with a given data subject. That data will be collected, held, and processed in accordance with the data protection principles (outlined below) and with this Notice in a reasonable and lawful manner. The types of information that the University may be required to handle include:

- Identification data – name, address, phone number, date of birth, gender and relevant national identification number
- Staff ID number & photograph
- Car registration
- Bank account details – sort code, account number and IBAN
- Pay and financial information (including tax and insurability classification)
- Emergency contacts
- Dependant data
- Prior work experiences and qualifications (such that might be normally associated with a CV)
- Awards received & professional membership information.
- Data relating to publications, invitations and other University's communications
- References

- E-mail addresses & relevant University IP addresses
- Marital status
- Gender
- Nationality
- Garda vetting data
- Phone numbers
- Contract of employment and commencement details
- Interview and selection notes
- Hosting or secondment agreements
- Various ongoing records that are generated in the course of your engagement (such as data relating to leave, training, performance reviews etc)
- Data required for the processing and progression of University Policies and Procedures (e.g. Human Resources policies)
- Health and Safety issues
- Health data (including medical certificates and reports regarding fitness to work and, where relevant vaccination records)
- Passports
- Visa and work permit details
- Driving licences
- Details relating to pension and various staff benefits
- CCTV

Some types of Personal Data are deemed to be Sensitive Personal Data, such as health or criminal conviction information. The University will only hold this information where the University has received your consent to do so, or for the purpose of your employment, or where otherwise lawfully permitted to do so. Illustrative examples of the use of categories of Sensitive Personal Data:

- Medical Information - for example, where special workplace accommodations are required to be considered or for compliance with the any sick leave scheme the University may procure medical reports, including Occupational Health Advisor reports, regarding staff. Such reports will contain Sensitive Personal Data regarding a staff member’s health status, conditions or illnesses.
- Criminal convictions – which may be processed in the context of appropriateness of employment or for disciplinary and grievance procedures.

Job Applicants

Job applications are received by the University, both solicited and unsolicited, either directly or via recruitment partners. There is no obligation on the University to retain or reply to unsolicited applications made. Unsolicited applications, whether in writing or via e-mail or other form *may* be issued with written notification from us upon receipt of your application and if and where relevant processed through the appropriate University Recruitment/Appointment Procedure. Applications sought by the University shall necessitate the furnishing of a range of Personal Data pursuant to the appropriate Recruitment/Appointment Procedure. The University will hold securely such applications and additional information which may be obtained during the course of any recruitment, interview and selection process, such as interview notes, education qualifications etc. electronically and/or manually. The general retention period for applications and interview notes is 18 months and documents are then securely destroyed, save for where applicants opt-in to retain data entered by them into the system in the course of their application, for ease of future applications made.

All provisions of this Notice will apply to the processing of your application. Your information may be shared with the University's agents or partners in connection with services that these individuals or entities perform. These agents or partners are restricted from using this data in any way other than to provide the specified related services (such as recruitment services or pre-employment and in-employment medical assessments for example).

Data Protection Principles

Anyone processing Personal Data (including the University) must comply with six core principles of good practice. These provide that Personal Data must be:

1. obtained and processed fairly, lawfully and in a transparent manner;
2. collected only for one or more specified and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. kept only to the extent that same is adequate, relevant and limited for what is necessary in relation to the purposes for which they are processed;
4. kept accurate and up-to-date;
5. retained no longer than is necessary for the purpose for which the data is processed; and
6. processed in a manner that is safe and secure.

The University is responsible for, and must be able to demonstrate compliance with the above principles.

Processing Personal Data

Personal Data collected by the University is collected in order to ensure that it can provide the best possible service to our students and wider stakeholders. It allows the University to work effectively with the its partners, associates and affiliates. The collection of that Personal Data allows the University to efficiently manage our employees, staff, contractors, agents and consultants. The

University uses staff Personal Data in its legitimate interests, for example in order to ensure it is able to administer staff contracts. It may also use Personal Data in meeting certain obligations imposed by law.

Business processes or staff administration uses for Personal Data include:

- recruitment, selection, promotion;
- reference and qualification checks;
- Garda vetting (or equivalent)
- changing salary;
- changing department/job code;
- changing working hours;
- terminating an employee contract;
- process offers of employment and processing work permits and visas where applicable;
- systems set up;
- processing payroll and tax;
- processing benefits and expenses;
- arranging travel visas;
- organising training programmes;
- initiating and progressing a University policy or procedure
- other reasons for ordinary personnel administration not listed here.

The University may also use your Personal Data to:

- assess performance and keep records of your development for the purposes of annual reviews, etc;
- communicate any changes to our policies, procedures or to your contract of employment (including changes to salary);
- contact you or your dependants if there are any health and safety or absence issues (including long term illness and maternity leave);
- calculate any changes in your salary; and/or
- retain contact information for the purposes of returning our property e.g. security cards, mobile phones, laptops, in connection with your departure from us.

Accuracy

The University shall employ reasonable means to keep Personal Data information accurate, complete and up to date in accordance with the purposes for which it was collected.

Staff are responsible for ensuring that they inform their Manager/Human Resources of any changes in their personal details. The University endeavours to ensure personal information held by it is up to date and accurate.

Staff Data Protection Privacy Notice

Staff Monitoring

Where the University provides e-mail facilities and access to the internet, same are provided in line with the policies and procedures of the University's Information Technology Division. Those policies and procedures are there to protect against the dangers associated with e-mail and internet use. They include a right to monitor e-mail and web usage. Please refer to the e-mail and internet usage policies for further details.

CCTV cameras are in operation at a range of points across the University campus and the primary purpose of having CCTV 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.

Does the University disclose information about you to anyone else?

Personal Data may be disclosed internally when passed from one department to another in accordance with the data protection principles and this Notice. Personal Data is not passed to any internal department or any individual that does not reasonably require access to that Personal Data with respect to the purpose(s) for which it was collected and is being processed. Sensitive and/or restricted staff information must have additional internal access restrictions as appropriate.

The University shall disclose staff information to third parties only when it is necessary as part of our operating practices or when there is a legal or statutory obligation to do so. Such third parties may include, but are not limited to:

- payroll, bank
- tax or pension advisors
- health insurers
- occupational health advisors
- trade union
- legal advisors

Whenever the University discloses staff information to third parties, it will only disclose that amount of personal information necessary to meet such business need or legal requirement. Third parties that receive staff information must satisfy the University as to the measures taken to protect the Personal Data such parties receive and to ensure compliance with the Legislation and this Notice.

Appropriate measures will be taken to ensure that all such disclosures or transfers of staff information to third parties will be completed in a secure manner and pursuant to contractual safeguards.

The University may provide information, in response to properly made requests, for the purpose of the prevention and detection of crime and the apprehension or prosecution of offenders. It may also provide information for the purpose of safeguarding national security. In the case of any such disclosure, we will do so only in accordance with the Legislation.

The University may also provide information when required to do so by law, for example under a court order.

The University may transfer data to legal counsel where same is necessary for the defence of legal claims.

In the event that there was any change in the ownership of any part of the University's operations or any of its assets, the University may disclose personal information to the new (or prospective) owner. If so, the University will require the other party to keep all such information confidential.

How long does the University keep personal information?

The time period for which the University generally retains information varies according to the use of that information. In some cases there are legal requirements to keep data for a minimum period of time. Unless specific legal requirements dictate otherwise, the University will retain information no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

The following is an illustrative guideline as to how long information of certain types are kept once you are no longer an employee of the University and is largely guided by legal factors:- Further information on the university's records management and retention policy is available at https://ulsites.ul.ie/corporatesecretary/records-management.

How would the University protect data about you were it to be transferred out of Europe?

Countries in the European Economic Area (EEA) are required to have a similar standard of protection of Personal Data. This is not always the case outside that area. In the event that the University would be required to transfer data outside the EEA (such as for a secondment), before doing so, steps would be taken to ensure that there is adequate protection as required by the Legislation.

How can you exercise your rights in respect of personal information the University holds about you?

The University shall vindicate all your rights under the Legislation. These rights are as follows:

- your right to request access to Personal Data held by the University, and to have any incorrect Personal Data rectified;
- your right to the restriction of processing concerning you or to object to processing;
- your right to have Personal Data erased (where appropriate); and
- your right to data portability regarding certain automated Personal Data
- with regard to rights within the Legislation relating to "automated decision-making", the University does not use such processes and they do not arise.

Vindication of your rights shall not affect any rights which we may have under the Legislation. If you want to exercise any right, you can do so by making your specific request in writing to the University's Data Protection Officer, Office of the Corporate Secretary, University of Limerick, Limerick. Your request will be processed within 30 days of receipt. If the information held about you is inaccurate, you are requested to advise the University promptly so that the necessary amendments can be made and same can be confirmed as being made within 30 days of receipt of your request. Staff also have the right to lodge a complaint with the Office of the Data Protection Commissioner.

How does the University protect personal information about you?

The University shall employ reasonable and appropriate administrative, technical, personnel, procedural and physical measures to safeguard staff information against loss, theft and unauthorised uses access, uses or modifications. All personal information stored is either password protected or is locked away in cabinets. Only a limited number of authorised personnel have access to this information.

The following principles apply:

- Confidentiality - only people who are authorised to use the data can access it.
- The University will ensure that only authorised persons have access to a staff personnel file and any other Personal or Sensitive Data held.
- Staff 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.
- Integrity - that the Personal Data is accurate and suitable for the purpose for which it is processed.
- Availability - that authorised users should be able to access the data if they need it for authorised purposes.

Staff Data Protection Privacy Notice

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.