St Patrick's Pontifical University
Maynooth
Co. Kildare
W23 TW77
(01) 7084700

Data Protection Policy

Title

Data Protection Policy of St Patrick's Pontifical University, Maynooth.

Introductory Statement

St Patrick's Pontifical University, Maynooth (hereafter, SPPU) Data Protection Policy applies to the personal data held by the University which is protected by the Data Protection Acts 1988 and 2003 and by EU General Data Protection Regulations 2018.

The policy applies to all SPPU staff, students and others (including prospective or potential students and their and applicants for staff positions within SPPU) insofar as the measures under the policy relate to them. Data will be stored securely, so that confidential information is protected in compliance with relevant legislation. This policy sets out the manner in which personal data and sensitive personal data will be protected by the University.

Data Protection Principles

St Patrick's Pontifical University is a *data controller* of *personal data* relating to its past, present and future staff, Students and other members of the University community. As such, SPPU is obliged to comply with the principles of data protection set out in the Data Protection Acts 1988 and 2003 and by EU General Data Protection Regulations 2018 which can be summarised as follows:

- **Obtain and process *Personal Data* fairly**: Information on Students is gathered at application and registration Information is also transferred from their previous University, if applicable. In relation to information the University holds on other individuals (members of staff, individuals applying for positions within the University, etc.), the information is generally furnished by the individuals themselves with full and informed consent and compiled during the course of their enrolment, employment or contact with the University. All such data is treated in accordance with the Data Protection Acts and the terms of this Data Protection Policy. The information will be obtained and processed fairly.

- **Keep it only for one or more specified and explicit lawful purposes**: The University will inform individuals of the reasons they collect their data and will inform individuals of the uses to which their data will be put. All information is kept with the best interests of the individual in mind at all times.

- **Process it only in ways compatible with the purposes for which it was given initially**: Data relating to individuals will only be processed in a manner consistent with the purposes for which it was gathered. Information will only be disclosed on a need to know basis, and access to it will be strictly controlled.

- **Keep *Personal Data* safe and secure**: Only those with a genuine reason for doing so may gain access to the information. Sensitive Personal Data is securely stored under lock and key in the case of manual records and protected with firewall software and password protection in the case of electronically stored data. Portable devices storing personal data (such as laptops) should be encrypted and password protected before they are removed from SPPU premises. Confidential information will be stored securely and in relevant circumstances, it will be placed in a separate file which can easily be removed if access to general records is granted to anyone not entitled to see the confidential data.

- **Keep Personal Data accurate, complete and up-to-date**: Students, dioceses/religious congregations/orders and/or staff should inform the University of any change which the University should make to their personal data and/or sensitive personal data to ensure that the individual's data is accurate, complete and up-to-date. Once informed, the University will make all necessary changes to the relevant records. The President may delegate such updates/amendments to

another member of staff. However, records must not be altered or destroyed without proper authorisation. If alteration/correction is required, then a note of the fact of such authorisation and the alteration(s) to be made to any original record/documentation should be dated and signed by the person making that change.

- **Ensure that it is adequate, relevant and not excessive**: Only the necessary amount of information required to provide an adequate service will be gathered and stored.

- **Retain it no longer than is necessary for the specified purpose or purposes for which it was given**: As a general rule, the information will be kept for the duration of the individual's time in the University. Thereafter, SPPU will comply with legislative guidelines on the storage of Personal Data and Sensitive Personal Data relating to a student. In the case of members of staff, SPPU will comply with both GDPR guidelines and the requirements of the Revenue Commissioners with regard to the retention of records relating to employees. SPPU may also retain the data relating to an individual for a longer length of time for the purposes of complying with relevant provisions of law and or/defending a claim under employment legislation and/or contract and/or civil law.

- **Provide a copy of their *personal data* to any individual, on request**: Individuals have a right to know what personal data/sensitive personal data is held about them, by whom, and the purpose for which it is held.

Scope

Purpose of the Policy: The Data Protection Acts 1988 and 2003 apply to the keeping and processing of *Personal Data*, both in manual and electronic form. The purpose of this policy is to assist SPPU with meeting its statutory obligations, to explain those obligations to SPPU staff and to inform staff, students and their dioceses/congregations/orders how their data will be treated.

The policy applies to all SPPU staff, students and others (including prospective or potential students, and applicants for staff positions within the University) insofar as the University handles or processes their *Personal Data* in the course of their dealings with the University.

Definition of Data Protection Terms

In order to properly understand the University's obligations, there are some key terms which should be understood by all relevant University staff:

Data means information in a form that can be processed. It includes both *automated data* (e.g. electronic data) and *manual data*. *Automated data* means any information on computer, or information recorded with the intention that it be *processed* by computer. *Manual data* means information that is kept/recorded as part of a *relevant filing system* or with the intention that it form part of a relevant filing system.

Relevant filing system means any set of information that, while not computerised, is structured by reference to individuals or by reference to criteria relating to individuals, so that specific information relating to a particular individual is readily, quickly and easily accessible.

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 that is in, or is likely to come into, the possession of the Data Controller i.e. the University.

Sensitive Personal Data refers to *Personal Data* regarding a person's:

- racial or ethnic origin, political opinions or religious or philosophical beliefs;
- membership of a trade union;
- physical or mental health or condition or sexual life;
- commission or alleged commission of any offence; or

- any proceedings for an offence committed or alleged to have been committed by the person, the disposal of such proceedings or the sentence of any court in such proceedings, criminal convictions or the alleged commission of an offence.

Data Controller for the purpose of this policy is the President, St Patrick's Pontifical University.

Rationale

In addition to its legal obligations under the broad remit of educational legislation, the University has a legal responsibility to comply with the Data Protection Acts, 1988 and 2003 and GDPR 2018.

This policy explains what sort of data is collected, why it is collected, for how long it will be stored and with whom it will be shared. As more and more data is generated electronically and as technological advances enable the easy distribution and retention of this data, the challenge of meeting the University's legal responsibilities has increased.

The University takes its responsibilities under data protection law very seriously and wishes to put in place safe practices to safeguard individual's personal data. It is also recognised that recording factual information accurately and storing it safely facilitates an evaluation of the information, enabling the President to make decisions in respect of the efficient running of the University. The efficient handling of data is also essential to ensure that there is consistency and continuity where there are changes of personnel within the University.

Other Legal Obligations

Implementation of this policy takes into account SPPU's other legal obligations and responsibilities. Some of these are directly relevant to data protection. ***For example:***

The Freedom of Information Act 1997 provides a qualified right to access to information held by public bodies which does not necessarily have to be "personal data" as with data protection legislation.

- Under *Children First: National Guidance for the Protection and Welfare of Children* (2011) published by the Department of Children & Youth Affairs, the University and staff have responsibilities to report child abuse or neglect to TÚSLA - Child and Family Agency (or in the event of an emergency and the unavailability of TÚSLA, to An Garda Síochána).

Relationship to characteristic spirit of SPPU (mission/vision/aims)

St Patrick's Pontifical University, Maynooth seeks to

- enable each student to develop his full potential;
- provide a safe and secure environment for study;
- promote respect for the diversity of values, beliefs, traditions, languages and ways of life in society.

We aim to achieve these goals while respecting the privacy and data protection rights of students, staff, dioceses/congregations/orders and others who interact with us. The University wishes to achieve these aims/missions while fully respecting individuals' rights to privacy and rights under the Data Protection Acts.

Personal Data

The *Personal Data* records held by the University **may** include:

A. ***Student records:***

(a) **Categories of student data**: These **may** include:

- Information which may be sought and recorded at enrolment and may be collated and compiled during the course of the student's time in the University. These records may include:
  - name, address and contact details;
  - PPS number;
  - date and place of birth;
  - religious belief;
  - racial or ethnic origin;
  - membership of the Traveller community, where relevant ;
  - whether they are medical card holders;
  - whether English is the student's first language and/or whether the student requires English language support;
  - any relevant special conditions (e.g. special educational needs, health issues etc.) which may apply.
- Information on previous academic record (including reports, references, assessments and other records from any previous University(ies) attended by the student;
- Character References;
- Professional References;
- Psychological, psychiatric and/or medical assessments;
- Attendance records;
- Photographs and recorded images of Students (including at University events and noting achievements);
- Academic record – subjects studied, class assignments, examination results as recorded on official University reports;
- Records of significant achievements;
- Records of disciplinary issues/investigations and/or sanctions imposed;
- Garda vetting outcome record (where the student is engaged in a pastoral placement organised with or through the University which requires that they be Garda vetted);
- Other records e.g. records of any serious injuries/accidents etc.;
- Records of any reports the University (or its employees) have made in respect of the student to State departments and/or other agencies under mandatory reporting legislation and/or child safeguarding guidelines.

(b) **Purposes**: The purposes for keeping student records are:

- to enable each student to develop to his full potential;
- to comply with legislative or administrative requirements;
- to ensure that eligible students can benefit from the relevant additional teaching or financial supports;
- to support the provision of education.
- to enable family to be contacted in the case of emergency or in the case of University closure;
- to meet the educational, social, physical and emotional requirements of the student;
- photographs and recorded images of students are taken to celebrate University achievements, compile yearbooks, establish a University website, record University events, and to keep a record of the history of the University. Such records are taken and used in accordance with the University's Data Protection Policy;
- to ensure that the student meets the University's admission criteria;
- to ensure that students meet the minimum age requirements for their course;
- to furnish documentation/ information about the student to the Department of Education and Skills and other institutes etc. in compliance with law and directions issued by government departments;
- to furnish, when requested by the student documentation/information/references to other third-level educational institutions and/or prospective employers;
- In respect of a pastoral placement, (where that work experience role requires that the student be Garda vetted) the University will assist the student in obtaining their Garda

vetting outcome (with the consent of the student) in order to furnish a copy of same (with the consent of the student) to the work experience employer.

(c) **Location**: In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.

(d) **Security:** These records are kept in manual record (personal file within a *relevant filing system*) and/or computer record (database) or both. Applicable security measures, e.g. locks, padlocks, password protection, firewall software, adequate levels of encryption etc. are in place.

C.. ***Other records:***

The University will hold other records relating to individuals. The format in which these records will be kept are manual record (personal file within a relevant filing system), and/or computer record (database). Some examples of the type of other records which the University will hold are set out below (this list is not exhaustive):

Charity tax-back forms

(a) **Categories of data**: the University may hold the following data in relation to donors who have made charitable donations to the University:

- name;
- address;
- telephone number;
- PPS number;
- tax rate;
- signature; and
- the gross amount of the donation.

(b) **Purposes**: Universities are entitled to avail of the scheme of tax relief for donations of money they receive. To claim the relief, the donor must complete a certificate (CHY2) and forward it to the University to allow it to claim the grossed up amount of tax associated with the donation. The information requested on the appropriate certificate is the donor's name, address, PPS number, tax rate, telephone number, signature and the gross amount of the donation. This is retained by the University in the case of audit by the Revenue Commissioners.

(c) **Location**: In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.

(d) **Security:** These records are kept in manual record (personal file within a *relevant filing system*) and/or computer record (database) or both. Applicable security measures, e.g. locks, padlocks, password protection, firewall software, adequate levels of encryption etc. are in place.

CCTV images/recordings

(a) **Categories**: CCTV is installed in some parts of the University, externally i.e. perimeter walls/fencing and internally as detailed in the CCTV Policy. These CCTV systems may record images of staff, Students and members of the public who visit the premises.

(b) **Purposes**: Safety and security of staff, Students and visitors and to safeguard University property and equipment.

(c) **Location**: Cameras are located externally and internally as detailed in the CCTV Policy. Recording equipment is located in the Security Office of St Patrick's Pontifical University, Maynooth.

(e) Security: Access to images/recordings is restricted to the President of SPPU. Tapes, DVDs, hard disk recordings are retained for 28 days, except if required for the investigation of an incident. Images/recordings may be viewed or made available to An Garda Síochána pursuant to section 8 Data Protection Acts 1988 and 2003.

Examination results

(a) **Categories**: The University will hold data comprising examination results in respect of its students. These include First Semester and End of Year Examinations.

(b) **Purposes**: The main purpose for which these examination results and other records are held is to monitor a student's progress and to provide a sound basis for advising them.

(c) **Location**: In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.

(d) **Security:** These records are kept in manual record (personal file within a *relevant filing system*) and/or computer record (database) or both. Applicable security measures, e.g. locks, padlocks, password protection, firewall software, adequate levels of encryption etc. are in place.

Links to other policies.

Our University policies need to be consistent with one another, within the framework of the overall University.. Relevant University policies already in place or being developed or reviewed, shall be examined with reference to the data protection policy and any implications which it has for them shall be addressed.

The following policies may be among those considered:

- Child Protection Policy;
- Dignity at Work and Study Policy;
- University Internet & Social Media Guidelines;
- Admissions Policy.

Processing in line with data subject's rights

Data in this University will be processed in line with the data subject's rights.

Data subjects have a right to:

(a) Request access to any data held about them by a data controller;
(b) Prevent the processing of their data for direct-marketing purposes;
(c) Ask to have inaccurate data amended;
(d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

Dealing with a data access requests

Section 3 access request

Under Section 3 of the Data Protection Acts, an individual has the right to be informed whether the University holds data/information about them and to be given a description of the data together with details of the purposes for which their data is being kept. The individual must make this request in writing and the data controller will respond to the request within 21 days.

The right under Section 3 must be distinguished from the much broader right contained in Section 4, where individuals are entitled to a copy of their data.

Section 4 access request

Individuals are entitled to a copy of their personal data on written request.

- The individual is entitled to a copy of their personal data (subject to some exemptions and prohibitions set down in Section 5 of the Data Protection Act);
- Request must be responded to within 40 days;
- Fee may apply but cannot exceed €6.35;
- Where a subsequent or similar request is made soon after a request has just been dealt with, it is at the discretion of the University as data controller to comply with the second request (no time limit but reasonable interval from the date of compliance with the last access request.) This will be determined on a case-by-case basis;
- No personal data can be supplied relating to another individual unless that third party has consented to the disclosure of their data to the applicant. Data will be carefully redacted to omit references to any other individual and only where it has not been possible to redact the data to ensure that the third party is not identifiable would the University refuse to furnish the data to the applicant.

Providing information over the phone

In our University, any employee dealing with telephone enquiries should be careful about disclosing any personal information held by the University over the phone. In particular the employee should:

- Check the identity of the caller to ensure that information is only given to a person who is entitled to that information
- Suggest that the caller put their request in writing if the employee is not sure about the identity of the caller and in circumstances where the identity of the caller cannot be verified
- Refer the request to the President for assistance in difficult situations. No employee should feel forced into disclosing personal information.

Implementation arrangements, roles and responsibilities

In our University, SPPU is the data controller and the President will be assigned the role of co-ordinating implementation of this Data Protection Policy and for ensuring that staff who handle or have access to *Personal Data* are familiar with their data protection responsibilities.

The following personnel have responsibility for implementing the Data Protection Policy:

Name:	**Responsibility:**
President:	Data Controller
Quality Assurance Manager	Data Champion
Executive Management Team:	Implementation of Policy

Teaching personnel:	Awareness of responsibilities
Administrative personnel:	Security, confidentiality
IT personnel:	Security, encryption, confidentiality

Ratification & communication

When the Data Protection Policy has been ratified by the Executive Management Team it becomes the University's agreed Data Protection Policy. It should then be dated and circulated within the University community. The entire staff must be familiar with the Data Protection Policy and ready to put it into practice in accordance with the specified implementation arrangements. It is important that all concerned are made aware of any changes implied in recording information on students, staff and others in the University community.

Students should be informed of the Data Protection Policy from the time of enrolment of the student e.g. by including the Data Protection Policy as part of the Application Pack, by either enclosing it or incorporating it as an appendix to the application form.

Monitoring the implementation of the policy

The implementation of the policy shall be monitored by the President.

At least one annual report should be issued to the Executive Management Team to confirm that the actions/measures set down under the policy are being implemented.

Reviewing and evaluating the policy

The policy should be reviewed and evaluated at certain pre-determined times and as necessary. On-going review and evaluation should take cognisance of changing information or guidelines (e.g. from the Data Protection Commissioner), legislation and feedback from Students, University staff and others. The policy should be revised as necessary in the light of such review and evaluation and within the framework of University planning.

Date: Updated as of 15th August 2024