Procedures for Data Protection

QA Area (s)	• Information and Data Management
Applies to	☐ Staff only ☐ Learners only ☒ Staff and Learners
Policies this Procedure relates to	Policy for Information and Data Management

1.1.1 Definition

Personal data is information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, by name, an identification number, location data, or an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1.1.2 Data Protection Management

The College will assign the management of personal data to a Data Protection Representative. The role will entail:

- Coordinating training to inform staff, faculty and associate faculty of the College of their obligations under GDPR.
- Coordinating the monitoring of compliance to GDPR with the assistance of external consultants and management as required.
- Alerting the Executive Management Team when Data Protection Privacy Impact Assessments are required.
- Reporting on matters related to Data Protection to the Executive Management Team.

1.1.3 Training

The College will implement a training programme covering data protection generally and the areas that are specifically relevant to the college.

Executive Management

The College will ensure all members of the management team are educated about their requirements under GDPR and the possible impact of non-compliance for the College.

The College will identify key senior management personnel to support the data protection compliance programme.

General Staff

The College will ensure all staff, faculty and associate faculty are provided with a training programme covering data protection generally and the areas that are specifically relevant to their jobs. The College will ensure refresher training is provided when required.

Attendance at all training courses will be recorded.

1.1.4 Privacy by Design

The College will adopt internal Technical and Organisational Measures to meet the principles of privacy by design and data protection by default. The College will implement technical and organisational measures by: -

- Implementing pseudonymisation and encryption where feasible
- Data Minimisation
- Risk Management
- Integrating data privacy into IT policies, Data Retention and Deletion Policy
- Providing data subject transparency and access
- By developing access controls for confidentiality which provide that only personal data which is necessary for each specific purpose of the processing is processed during the retention period as informed to the data subject
- By developing access controls (roles-based) which provide that personal data is not made accessible to more individuals than necessary for the purpose
- Providing an audit trail of the access controls
- Ability to restore availability of and access to data in the event of an incident
- Regular test of the effectiveness of security measures

The College will take all reasonable steps to ensure that appropriate security measures are in place to protect the confidentiality of both electronic and manual data. Security measures will be reviewed periodically and where necessary, having regard to the technology available, the cost and the risk of unauthorised access.

Employees must implement all organisational security policies and procedures,

- use of computer passwords,
- automatic screensavers,
- locking filing cabinets,
- clean desk policy,
- data minimisation and paperless policy.

Employees must play their part in ensuring its Data Subjects' confidentiality. They must adhere to the following data protection principles:

- Process data fairly, lawfully and transparently.
- Keep data only for specified, explicit and legitimate purpose.
- Process data only in ways which are compatible with the purpose(s) for which it was given.
- Ensure data is accurate and up-to-date.

- Ensure data is adequate, relevant and limited to what is necessary for the purpose for which it was given.
- Keep data safely and securely.
- Retain personal data for no longer than is necessary for the purpose for which it is processed and in line with the College data retention policy.
- Employees must not disclose personal data, except where necessary in the course of their employment, or in accordance with law.
- They must not remove or destroy personal data except for lawful reasons and with the permission of the organisation.

Any breach of the data protection principles is a serious matter and may lead to disciplinary action up to and including dismissal. If employees are in any doubt regarding their obligations, they should contact the data protection guidelines the Data Protection Representative.

1.1.5 Data Privacy Impact Assessment (DPIA)

The College will carry out privacy impact assessments where a type of processing is likely to result in a high risk for the rights and freedoms of data subjects in the following cases but not limited to this list: -

- in the event of a systematic monitoring of a publicly accessible area
- in the context of profiling on which decisions are based that produce legal effects
- in the event of implementing new IT which infringes on the data subject's rights
- in the event there is a change to the risks posed by the processing operations to personal data

The College will have in place a process for determining whether a Data Privacy Impact Assessment (DPIA) is required. A DPIA will be embedded in all Business Cases presented to management for any proposed new projects.

If a DPIA is required, the following process will be conducted: -

- a systematic description of the processing operations and purposes of the processing
- an assessment of the necessity and proportionality of the processing operations
- an assessment of the risks to the rights and freedoms of data subjects
- if appropriate may seek the views of the affected data subjects
- measures envisaged to address the risks

The College will consult the Supervisory Authority (Data Protection Commissioner) if a DPIA result is of a high level of risk where the College cannot take measures to mitigate this risk.

1.1.6 Demonstrating Consent

The College will have an audit trail for consent. This will demonstrate that consent was given when relying on consent as grounds for processing personal data. Given the nature of the services offered consent is predominately relied on prior to engagement letters signed by the learner at the enrolment stage.

Consent is recorded from all data with a clear record of what each individual data subject consented to.

1.1.7 Demonstrating Compliance to the data protection principles

The College will document all the current processing activities to provide a Personal Data Register Data Protection Register identifying: -

- Service Department and Service line
- Data Class and Data Category
- Process Name
- Purpose for processing
- Controller/Processor/Both/Joint Controller
- Data Owners
- Lawful basis
- Data Accuracy Process
- Process Map where available
- Format of Data
- Recipients of Data
- Data shares internally and lawful bases provided
- Transfer methods
- Location of Data storage
- Retention Periods
- Data Access Controls
- Risk Management
- Transfers to Third Countries
- External Processor

The College will update its current policies and procedures to ensure compliance to the principles.

1.1.8 Records to be maintained as a Data Controller

The College will: -

- clearly identify where personal data is processed within the company, including by third party processors.
- provide the name and contact details of the College's Data Protection Representative and any joint controller.
- use the Personal Data Register to record details of:
    - the purposes of the processing.
    - a description of categories of data subjects and personal data.
    - the categories of recipients of personal data.
    - the details of transfers to third countries.
    - the time limits for erasure of different categories of data.
    - a general description of technical and organisational security measures taken.

1.1.9 Records to be maintained as a Processor

The College will use the Personal Data Register to record the following details in respect of any partner (controller)

- name and contact details of the partner (controller) on behalf of which it is processing.
- categories of processing.
- transfers of data to a third country or international organization.
- general description of the technical and organisational security measures.

As part of data accuracy, the College will keep information relating to the contracts that they are responsible for up-to-date and accurate.

1.2 Joint Controller Agreements

In circumstances where the College and another organisation determine the purposes for which and the way the personal data is processed, each party will be a controller and will be liable for the entirety of any damage to a data subject, unless they can prove they were not in any way responsible for the event giving rise to the damage.

The College will ensure that there is a clear attribution of data protection responsibilities between joint controllers and that this information is made available to data subjects through privacy notices or other means so that a controller will be able to show it was in no way responsible for the event giving rise to the damage if this is the case.

The College will ensure that contract negotiators are aware of the default position of each controller being liable for the entire damage to a data subject if it is in any way responsible for the event giving rise to the damage and include appropriate cross indemnification.

Once our applicants become students of the College, the College will share their information with TU Dublin and Griffith College and Springboard where necessary and appropriate.

All Data Subjects will be made aware of the College relationship with Springboard, TU Dublin and Griffith College. To ensure transparency for our Data Subjects we have a Code of Conduct which students must read and sign.

1.2.1 The Code of Conduct - includes

- A section for them to advise them of the data sharing between TU Dublin and Griffith College and it explicitly refers them to the College, TU Dublin and Griffith College Privacy Policy for further information should they want to read it.
- A notice to advise that at each class we will circulate a sign-in sheet for them to record their attendance on.
- We would also refer our data subjects to the privacy policies of the 3rd parties with whom we share their personal data.

  - Technological University Dublin https://www.it-tallaght.ie/gdpr
  - Griffith College https://www.griffith.ie/offices/data-protection

1.2.2 Processors

For all their partners who are legal entities. The College as a processor will ensure: -

- to implement Technical and Organisational Measures (TOM) to safeguard the personal data.
- not to appoint sub- processors without the consent of the controller.
- to notify breaches to the controller.
- to cooperate directly with the Supervisory Authority.
- to assess any intra-group processor agreements and make amendments to include minimum requirements and if necessary, to keep liability limited towards the group's main establishment or service companies.

1.3 Budget

The College will allocate an annual budget for data protection compliance.

1.4 Reporting

Staff are required to report any data breaches to the Data Protection Representative as soon as the data breach is discovering (regardless of the timing of the discovery, including the day of the week and time of the day).

The Data Protection Representative will report to all staff any new changes to GDPR and any cyber threats or attacks as this information becomes known. The College will also provide staff with steps to take to avoid this occurring to the College.

The Data Protection Representative will report to management monthly on: -

- Internal incidences reported.
- Internal breaches.
- GDPR improvements implemented.
- Status of current projects on GDPR.
- Awareness and training process.
- Relevant external breaches reported.
- Updates to compliance.
- DPIA's.

The Data Protection Representative will assess all data breaches reported in line with the data breach policy and if such a breach requires reporting to the Supervisory Authority, this will be approved by management.

1.5 Data Protection: Organisation

1.5.1 11.7.1 Definitions

Data – Information, which is stored electronically, on a computer, or in certain paper-based filing systems. This includes IT systems and CCTV systems.

Data Subjects - For the purposes of this document includes all living individuals about whom the College holds personal data.

Personal Data – Data relating to a living individual who can be identified from the data (or from that data and other information that is in, or likely to come into the possession of the data controller). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

Data controllers – The individuals or organisations who control and are responsible for keeping and use of data.

Data users – Employees whose work involves using personal data. Data users have a duty to protect the information they handle by following the College's data protection security policies at all times.

Processing – Performing any operation or set of operations on data including: -

- Obtaining, recording or keeping data.
- Collecting, organising, storing, altering or adapting the data.
- Retrieving, consulting or using the data.
- Disclosing the information or data by transmitting, disseminating or otherwise making it available.
- Aligning, combining, blacking, erasing or destroying the data.

Sensitive personal data – Information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health condition or sexual life, criminal convictions or the alleged commission of an offence. Sensitive personal data can only be processed under strict conditions and will usually require the express consent of the person concerned.

1.5.2 Data Protection Principles

Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be: -

a) Obtained and processed fairly

GDPRs are intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the Data Protection Contact is, the purpose for which the data is to be processed by the College and the identities of anyone to whom the data may be disclosed or transferred.

For personal data to be processed lawfully, certain conditions must have been met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

b) Kept only for one or more specified, explicit and lawful purposes

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for other purposes specifically permitted

by GDPR. This means that personal data must not be collected for one purpose and used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs. Any employee personal data collected by the College is used for ordinary Human Resources purposes. Where there is a need to collect employee data for another purpose, the College will notify the employee of this and where it is appropriate will get employee consent to such processing.

c) Used and disclosed only in ways compatible with these purposes

Personal data should only be collected to the extent that it is required for the specific purposes notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

d) Kept safe and secure

The College and its employees must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

GDPR require the College to put in place procedures and technologies to maintain the security of all personal data. Personal data may only be transferred to a third-party data processor if the third party has agreed to comply with those procedures and policies or has adequate security measures in place.

The following must be maintained: -

- Confidentiality – Only people authorised to use the data can access it. The College will ensure that only authorised persons have access to an employees' personal file and any other personal or sensitive data held by the College's employees are required to maintain the confidentiality of any data to which they have access.
- Integrity – Personal data is accurate and suitable for the purpose for which it is processed.
- Availability – Only authorised users should be able to access the data if they need it for authorised purposes

Security Policy / Procedures include: -

- Secure lockable desks and cupboards. - Clear desk policy, all desks and cupboards remain locked when not in use. Personal information is always considered confidential and treated with extra precautions, ensuring no one can see work that contains the same.
- Methods of disposal. – Paper documents must be shredded. All removable media should be wiped and physically destroyed when no longer required.
- Equipment – Data users should ensure that individual monitors do not show confidential information to passers-by and that the screen saver starts as soon as their PC is unattended.

e) Kept accurate, complete and up to date

Personal data must be accurate and kept up to date. Information which is incorrect, or misleading is not accurate, and steps should be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate

or out-of-date data should be destroyed. Employees should ensure that they notify the Data Protection Contact and College Administration of any relevant changes to their personal information so that it can be updated and maintained accurately. Examples of relevant changes to data would include a change of address.

f) Adequate, relevant and not excessive

g) Retained for no longer than is necessary for the purpose or purposes for which it was collected

Personal data should not be kept longer than is necessary for the purpose. For guidance in relation to data retention employees should contact their manager. The College has various legal obligations to keep certain employee data for a specified period. In addition, the College may need to retain personal data for a period to protect its legitimate interests.

h) Provided to data subjects as requested

Data must be processed in line with data subject's rights. Data subjects have a right to: -

- Request access to any data held about them by the Data Controller.
- Prevent the processing of their data for direct marketing purposes.
- Ask to have inaccurate data amended.
- Prevent processing that is likely to cause or distress to themselves or anyone else.

1.5.3 Dealing with Subject Access Requests

A formal request from a data subject for information that the College holds about them must be made in writing. Any employee who receives a written request in respect of data held by the College should forward it to the Data Protection Representative.

Under the EU General Data Protection Regulation (GDPR) Article 15, data subjects have the right to access and obtain a copy of any personal data held on them by an organization. Data Access Requests (DAR) also known as Subject Access Requests (SAR) may be made verbally or in writing. According to GDPR, any data requests made must be acted upon **"without undue delay"** and completed within 28 days from the date of the request.

Where the College has received a verbal or written request for data access the following specific steps must be followed in order to ensure the request is dealt with appropriately and in an effective manner.

The Data Access Request process is coordinated by the Data Protection Representative (DPR). The ultimate responsibility to conduct a search and collation of non-sensitive or organizational data following a request, resides with the DPR, who may as part of this process delegate or task fellow employees to complete parts of this process.

Note: DPR must satisfy themselves as to the comprehensive completion of this process.

1.5.4 Steps in the Data Access Process

1. Receipt of a Data Access Request.
2. From the date the request is received, the College has 28 days to respond to and complete the request in full.
3. The request is immediately forwarded to the College's Data Protection Representative and to the GDPR department email: gdpradmin@Innopharmalabs
4. The DPA creates a file for the data access request in the GDPR folder and the data request is recorded.
5. DPR Contacts Data Subject and Confirms Request
6. No later than 2 days from the request being made, the DPR is to contact the data subject and confirm the request as well as outlining to the data subject the process for dealing with the request and advise that the College has 28 days to complete the action. At this point, the data subject should also be made aware of the existence of their right to request from the College rectification or erasure of any data held on them by the College.

1.5.5 DPR Coordinates Data Search

- The DPR to conduct and coordinate the search of the College's data base systems. Employees may be delegated specific tasks to assist in the process.
- All data sources both soft and hard copy, must be included in the database systems review and searched thoroughly for any data pertaining to the data subject.
- Employees to send this data back on to the DPA.

Hard Copy

- Hard copy data may be stored on desks and in cabinets and include the following:
    - Invoices, delivery dockets, vendor details. non-disclosure agreements, business contracts, engineering reports, lead forms, personal notebooks.

Soft Copy

- Zoho - CRM, Campaign, Sales IQ
- Il-Server - shared folders, personal folders, backup server
- Microsoft Exchange, Sharepoint, One Drive – shared folders, personal folders
- Personal Laptops
- Mobile phones
- External storage devices
- Employees will be asked to perform a Windows document search on one drive and locate any relevant data files which are then sent back to the DPA.

1.5.5.1 Restrictive or Sensitive Data

Where data pertaining to the data subject resides in documents with other information of a sensitive or restrictive nature, such as Confidentiality Agreements or where personal details pertaining to another individual are also contained, then such information in that document is redacted. Such a decision would be up to the judgement and discretion of the DPA to make the call. In the case where any information in a document is redacted, a legitimate reason must be provided.

1.5.5.2 DPA to collate data

On receipt of all relevant data files, the DPA to compile the data in single coherent document and a copy sent to the data subject no later than 28 days from the date of the request.

1.5.5.3 File All Request Details and Correspondence

All communication and documentation relating to the data subject's request should be filed in relevant folder for audit trail purposes and for future reference if necessary.

1.5.5.4 Obtain Acknowledgment from Data Subject After Completion

Every reasonable effort is made to obtain acknowledgment from the data subject that the request is completed to their satisfaction.

1.5.6 Policy Review

This data protection notice will be reviewed from annually to take into account changes in the law and the experience of the notice in practice.

1.5.7 Providing Information Over the Telephone

Any employee dealing with telephone enquiries should be careful disclosing any personal information held by the College over the phone. 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 their manager and/or the Data Controller for assistance in difficult situations. No employee should feel forced into disclosing personal information.

1.6 *Data Protection: Employees*

1.6.1 HR What are your rights under data protection law?

You have the following rights under data protection law, although your ability to exercise these rights may be subject to certain conditions. It may be still lawful for us to continue processing your information even where you have withdrawn your consent, if one of the other legal bases is applicable.

- the right to receive a copy of and/or access the personal data that we hold about you, together with other information about our processing of that personal data;
- the right to request that any inaccurate data that is held about you is corrected, or if we have incomplete information you may request that we update the information such that it is complete;
- the right, in certain circumstances, to request that we erase your personal data;

- the right, in certain circumstances, to request that we no longer process your personal data for particular purposes, or object to our use of your personal data or the way in which we process it;
- the right, in certain circumstances, to transfer your personal data to another organisation;
- the right to object to automated decision making and/or profiling; and
- the right to complain to the Data Protection Commissioner.

1.6.2 Review of HR GDPR

This data protection notice will be reviewed from time to time to take into account changes in the law and the experience of the notice in practice.

1.6.3 Further information

If you have any queries in relation to this data protection notice, or if you have any concerns as to how your data is processed, please contact your Manager.

1.6.4 Data Retention Policy with Respect to Employee Records

This policy and schedule has been put in place to ensure that personal data is only retained for as long as is necessary for the purpose for which it was given to the organisation. The policy ensures respect for the data privacy of employees, lessens the risk of a data breach and aims to prevent loss of personal data.

Employees are obliged to have a clear awareness of the data retention policy and, where they are responsible for relevant data, to implement the retention periods set out below.

Recruitment related data	Contact details, date of birth, curriculum vitae, work and educational history, referee names, interview notes, related documentation etc	Individuals have 12 months to refer a complaint to the Workplace Relations Commission under the Employment Equality Acts 1998-2015, therefore this documentation will be retained for at least 12 months from the date the position is filled in order to defend any claim to the WRC.
Terms and conditions of employment	Personal data contained in contracts of employment and all related documentation	The Terms of Employment (Information) Act 1994-2012 provides that an employee's terms and conditions of employment must be retained for the duration of the employment and 1 year thereafter. The statute of limitations provides that a claim for breach of contract may be brought up to 6 years from the date of breach. Plaintiffs have 1 year from the commencement of proceedings on a defendant.

		Therefore, all contractual and related documentation will be retained for the duration of employment and 7 years from the termination or expiration of the contract.
Working time records	Weekly working hours, annual leave and public holidays, rest breaks, PPS numbers, statement of duties, name/address of each employee, copy of employment contract, copy of any notices given to employee about starting and finishing times and notice of additional working hours.	The Organisation of Working Time Act 1997 and related regulations provide that working time records must be retained for a minimum 3 years from the date of creation.
Payslips		The National Minimum Wage Act 2000 provides that payslips must be retained for at least 3 years from the date of their making.
Employee payroll and tax records		To comply with Revenue requirements all employee and tax records be retained for 7 years from the end of the financial year following termination of employment to the end of any enquiry by the Revenue Commissioners.
Employment Permit Records	Duration of employment, remuneration details, employment permit details	The Employment Permits Act 2003-14 provides that employment permit records must be retained for 5 years or a period equal to the duration of employment.
Parental Leave/force majeure leave records	Commencement of leave, duration of leave, manner in which leave was taken, notices and employee signatures	The Parental Leave Acts 1998 and 2006 provide that records must be retained for 8 years from the date of the leave. Notices in relations to the leave must be retained for 12 months.
Paternity leave records	As above	The Paternity Leave and Benefits Act 2016 provides that records of the leave taken must be retained for 8 years.
Carer's Leave Records	As Above	The Carers Leave Act 2001 provides that records of the leave taken must be retained for 8 years. Notices in relation to the leave must be retained for 3 years.

Records of employees under 18 years of age	Written permissions from parent/guardian, name, date of birth, starting and finishing times of work, pay details	The Protection of Young Persons (Employment) Act 1996 provides that records must be retained for at least 3 years
Medical Records	Sick leave certificates, occupational health assessments and any other records relating to sick leave.	the College recommended to keep for 7 years
Email and internet usage	Emails stored in an employee's email inbox and data relating to an employee's internet browsing history.	IT have access to employee's emails where necessary in the interest of the business.
CCTV usage	the College has closed circuit television cameras located on the ground floor of the College in the lobby beside the elevator and the reception area. This is necessary in order to protect against theft or pilferage, for the security of staff and organisation property. Access to the recorded material will be strictly limited to authorised personnel. Please refer to the CCTV policy for further details.	CCTV Policy states that all recordings are maintained on a weekly basis. This is necessary in order to protect against theft or pilferage, for the security of staff and organisation property. Access to the recorded material will be strictly limited to authorised personnel.

All retention periods set out above are subject to the data protection principles applicable to the personal data contained in records.

1.6.5 Extension of retention periods

The retention periods set out above may be extended in exceptional circumstances including where records are required by the organisation to defend any legal claims taken against it or on receipt of appropriate advice.

1.6.6 Security of data

The organisation will take all reasonable steps to ensure that appropriate security measures are in place to protect the confidentiality of data being destroyed in line with this retention policy.

1.7 Data Retention: Students

The College retains personal data indefinitely for all past and active students in accordance with our legitimate business needs, except if specifically requested by the data subject to remove their data from our records, in which case we will action this request in accordance to our data deletion procedure.

For those subjects who are coming to us via Springboard, the College have a statutory obligation to report to Springboard on these subjects regarding their academic and employment status/outcomes, therefor even if a data deletion request is made there will be information we must hold as part of our legal obligations, we will also hold the data to support the data deletion request.

1.7.1 The personal data we collect from you

Enquiries and leads

When you request information or make enquiries about any of our services or programmes, we may use the personal data you provide in order to fulfil your request or respond to your enquiry. So that we can provide you with the information, courses, programmes or services, you have requested, we collect and store certain information about you, including your name, telephone number, e-mail address, postal address and educational background when you ask for information about our courses or study materials. It is in our legitimate interests to use your personal data in this way so that you receive the information you have requested.

Applications and Enrolments

If you are applying or enrolling as a student, we may collect the following personal data about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth.
- Gender.
- Nationality and country of residence.
- Education history.
- Employment history (if applicable).
- Personal Public Service (PPS) number (if applicable).
- Official Photo Identification
- Credit card or other payment information in order to process your payments.

This information will be used by us to perform the contract we have entered into with you.
We may also collect information about your academic experience and progression. This is in order to fulfil our contract with you but it is also in our legitimate interests to use this personal data in order to monitor the provision of our service to you.
We may also collect personal data about your health in order to make appropriate arrangements and reasonable adjustments for you regarding your welfare or attendance. We use this information in order to perform our contract with you and in order to comply with our legal obligations.
We also may collect from you emergency contact information, such as the telephone number or email address for a friend or family member. By submitting such data to us, you represent to us that you have obtained consent from your emergency contacts to provide us their information for this purpose.

Marketing

Where you have explicitly consented to do so, we may use your personal data to:

1. Inform you of new information that we believe may be of interest to you and the programme area(s) you have shown the interest in; and/or

2. Invite you to Open Events or Information Sessions relevant to your programme(s) of interest.
3. If you would prefer that we do not send such communications to you, please follow the opt-out links on any marketing message or contact us using the contact details in this Privacy Notice.

Internal business purposes

We also may use your personal data for our internal business purposes. This is in our legitimate interests in order to operate as a business and monitor and improve the services we provide. Where possible we will anonymise this information. Please contact us using the contact details in this Privacy Notice if you would like more information.

Automated technologies or interactions.

As you interact with our website, we may automatically collect technical data about your equipment, browsing actions and patterns. We collect this personal data by using cookies and other similar technologies. Please see our cookie policy on our website for further details.

If you fail to provide personal data

Where we need to collect personal data by law, or under the terms of a contract we have with you and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you (for example, to provide you with goods or services). In this case, we may have to cancel a product or service you have with us but we will notify you if this is the case at the time.

When and how we share your personal data with others

We may share your personal data with third parties where required by law, where it is necessary to perform a contract or where we have a legitimate interest in doing so. We will need to use your data to perform our obligations and exercise our rights under agreements made with you and to inform you of feedback and exam results.

Awarding Bodies: We provide certain personal information collected by us, including PPS numbers, to Quality and Qualifications Ireland (QQI) and other Awarding Bodies to allow them to process students' results through their systems Privacy Statement.

Such third parties may include the following:

- Our service providers: We may share your personal data with other companies that perform certain services on our behalf. These services may include legal, financial and accounting advice, processing payments, providing customer service and marketing assistance, performing business and sales analysis and supporting our website and IT functionality. These service providers may be supplied with or have access to your personal data solely for the purpose of providing these services to us or on our behalf. Innopharma Education is the data controller and will remain accountable for your personal data.

- Your employer or potential employer: We may share your personal data with your employer or potential employer with whom we have a contract relating to your programme of study. This may include attendance and exam results.
- Awarding Bodies: We provide certain personal information collected by us, including PPS numbers, to Quality and Qualifications Ireland (QQI) and other Awarding Bodies to allow them to process students' results through their system.
- Public Health Officials: We are obliged to provide contact information to the Department of Health and/or the Health Service Executive for the purpose of contact tracing in the event that a case of COVID-19 or another infectious disease is reported amongst the Innopharma community.
- Others: We may share your personal information with other third parties such as in the context of the possible sale of our business. We may also need to share your personal data in order to permit us to pursue available remedies or limit damages we may sustain.

1.7.2 Innopharma Education – Data Retention Schedule

This retention schedule provides a guideline on how long Innopharma Education records should be retained under the current Records Management Policy. This Schedule ensures that information is kept as long as necessary and takes account of our responsibility to be compliant with the Data Protection Act. When retention periods for records have expired, documents should be reviewed in accordance with the college's Retention and Destruction policy, which has been included in this schedule. Where a retention period has expired electronic documents will be deleted and hard copies of documents will be confidentially shredded.

Where it is believed that there is justification to retain the data longer than indicated, then explicit reasons should be documented for doing so in consultation with the head of department or line manager.

Head of Academic Affairs Office

Document/record	Retention period	Action	Responsible
General Information Files containing a wide range of materials pertinent to the operation and interest of the Registrar's office.	Indefinitely		Director of Academic Affairs
Minutes of Meetings	Indefinitely		Director of Academic Affairs
New course approvals, process and reports	Indefinitely		Director of Academic Affairs

Circular letters and Government Reports	Indefinitely		Director of Academic Affairs
Documents and correspondence relating to litigation or disputes which have been completed or settled.	7 years	Delete all electronic files. /Shred hard copies	Director of Academic Affairs
Prospectus, Student Handbooks, Graduation Booklets	Indefinitely		Director of Academic Affairs
Programmatic Review Documents/Institutional Reviews	Indefinitely		Director of Academic Affairs
Disciplinary Committee Minutes	7 years after completion of event.	Delete all electronic files. /Shred hard copies	Director of Academic Affairs
Student Discipline Records -Major Offences	Duration of programme + 7 years, if a matter of public importance may be kept longer.	Delete all electronic files. /Shred hard copies	Director of Academic Affairs

Academic Council

Document/record	Retention period	Action	Responsible
Signed minutes of meetings and backup material of Academic Council meetings, details of its sub	7 years	Delete all electronic files. /Shred hard copies	Secretary of Academic Council

committees and working groups.			
General correspondence	3 years	Delete all electronic files. /Shred hard copies	Secretary of Academic Council
Approved programme schedules	indefinitely		Secretary of Academic Council

Education Management Committee

Document/record	Retention period	Action	Responsible
Signed & Approved minutes of meetings and supporting documentation	7 years	Delete all electronic files. /Shred hard copies	Secretary of Education Management Committee

Quality Assurance Enhancement Office

Document/record	Retention period	Action	Responsible
Minutes of meetings of academic council sub-committees, backup materials	7 years	Delete all electronic files. /Shred hard copies	Head of Quality Assurance
Procedure & guideline document master copies and approval records	7 years	Delete all electronic files. /Shred hard copies	Head of Quality Assurance
Collaboration Agreements etc.	Permanent		Head of Quality Assurance

Admissions

Document/record	Retention period	Action	Responsible
Direct Applications - (Unsuccessful/Not accepted) & opt out of Marketing.	18 months	Delete all unsuccessful applications from Zoho	Admission Coordinator
Direct Applications - (registered)	Duration of programme + 3 years	Removing from Zoho	Admission Coordinator
Registration Forms	Duration of programme + 3 years	Removing from Zoho	Admission Coordinator
Learner Personnel files including those of withdrawn learners.	Duration of programme + 2 years	Removing from Zoho	Admission Coordinator
Learner Statistics – academic/progression/career outcomes	Indefinitely		Admission Coordinator
Student records relating to tuition fees	Duration of programme + 3 years	Removing from Zoho	Admission Coordinator
Learner Record Forms	Duration of programme + 2 years	Remove from Zoho	Admission Coordinator

Registrations

Document/record	Retention period	Action	Responsible

Basic Student Registration details	indefinitely, unless the student raises an objection to same		Admission Coordinator
Medical Cert/Absence record	Duration of programme + 3 years	Delete all electronic files. /Shred hard copies	Admission Coordinator Admission Coordinator
I.D. Card Record	Duration of study	Delete all electronic files. /Shred hard copies	Admission Coordinator
Graduation In Absentia payment file	Indefinitely		
Course Timetabling Record	2 Years	Delete all electronic files. /Shred hard copies	Admission Coordinator

Examinations

Document/record	Retention period	Action	Responsible
Minutes of internal meeting	7 Years	Delete all electronic files. /Shred hard copies	Examination's office
Examinations papers & associated solutions	Indefinitely		Examination's office

deferral, withdrawal and applications for transfer course	Duration of programme + 3 years	Delete all electronic files. Removal from Zoho	Examination's office
Student Discipline Records -Major Offences	Duration of programme + 3 years	Removal from Zoho	Examination's office
Examination scripts	1 year following the Autumn repeat cycle of the year in which the exam was held.	Shred Hard Copy Scripts and Delete Electronically held assessments.	Examination's office
Assessment results - broadsheets	Indefinitely		Examination's office
Examination results - individual module sheets provided by external and internal examiners	Indefinitely		Examination's office
Examination Appeals documentation	3 years after the student ceases to be a registered student at the College provided no litigation is initiated during that period.	Delete from Record and One drive	Examination's Office
General correspondence	2 years after the student ceases to be a registered student of the College	Delete from Record and One drive	Examination's Office
External Examiner report & Records of exam board meetings Assessment results	Indefinitely		Examination's office
Conferring records	Indefinitely		Examination's office

Invigilator C.V.'s	18 months	Delete Electronic Copies & Shred hard copies	Examination's office
Repeat Exam Application records	Duration of programme + 2 years	Delete Electronic Copies	Examination's office
Requests for Transcripts/Parchments	6 months from completion of task	Delete Electronic Copies	Examination's office
Student records including academic outcomes.	Indefinitely		Examination's office

Student Services

Document/record	Retention period	Action	Responsible
Minutes of meeting	Indefinitely		Student Services Coordinator
Student information relating to support/library enrollment/general.	2 years after the student ceases to be a registered student of the College.	Delete Electronic Copies	Librarian
Student correspondence – emails/letters	2 years after the student ceases to be a registered student of the College.	Delete Electronic Copies	Student Services Coordinator
Student information to set up library accounts is transferred from the Banner database system.	Duration of course plus 1 year	Delete Electronic Copies	Librarian
Borrowing Records	Duration of course plus 1 year	Delete Electronic Copies	Librarian

Undergraduate dissertations (Thesis), Post Graduate Dissertations, Theses research and Taught Masters	Indefinitely		Librarian

IT Service

Document/record	Retention period	Action	Responsible
Minutes of meeting	Indefinitely		IT Services Manager
Attendance Records	1 year	Delete electronic record.	IT Services Manager
Student Moodle records	2 years after the student ceases to be registered in the college.	Record archived 2 semesters after completion and deleted thereafter in accordance with retention period	IT Services Manager
Lecture Recordings	2 years	Attached to Moodle record and deleted in line with Moodle record retention period.	IT Services Manager
Staff Accounts	Immediate after staff exit	Delete record – Moodle , All Microsoft access (one drive, SharePoint email)	IT Services Manager
CCTV	2 weeks	Auto resets every 2 weeks	IT Services Manager

HR

Document/record	Retention period	Action	Responsible

Personal Records - employment history, qualifications, training, salary increments, appointment details, medical certificates, leave of absence, birth certificates, staff development, etc.	Term of Employment plus 6 years	Delete Electronic Files/Shred hard copy files	HR Manager
Interview Report Forms, Selection Board recommendations. Application forms and any other documentation in respect of applicants who are not offered positions	12 months from the date the position is filled in order to defend any claim to the WRC.	Delete Electronic Files/Shred hard copy files	HR Manager
HR Policies and Procedures	Indefinitely		HR Manager
Attendance Records - Sick leave, annual leave, maternity leave, Force Majeure, Parental Leave etc.	Term of Employment plus 3 years Term of Employment plus 8 years	Delete Electronic Files/Shred hard copy files	HR Manager
Training: Details of courses attended; Training Budget and related correspondence. Applications for support subsidy, Training Policy	Indefinitely		HR Manager
Staff lists, addresses and contact numbers	Duration active employment and updated on an ongoing basis	Delete Electronic Files/Shred hard copy files	HR Manager

General Correspondence	3 Years	Delete Electronic Files/Shred hard copy files	HR Manager

Finance

Document/record	Retention period	Action	Responsible
Insurance documentation	7 years	Delete Electronic Files/Shred hard copy files	Finance Manager
Budget files and correspondence	Indefinitely		Finance Manager
Signed financial statements and audit reports	Indefinitely		Finance Manager
Final operating programme and budgets	10 years	Delete Electronic Files/Shred hard copy files	Finance Manager
Internal audit reports	10 years		Finance Manager
Legal documents and correspondence	Indefinitely		Finance Manager
All payroll reports for weekly, monthly and part-time staff	3 Years	Delete Electronic Files/Shred hard copy files	Finance Manager
Memos from personnel for payroll calculations	6years	Delete Electronic Files/Shred hard copy files	Finance Manager
P35s and P30s and P60s	6years	Delete Electronic Files/Shred hard copy files	Finance Manager

Bank statements	6years	Delete Electronic Files/Shred hard copy files	Finance Manager
Bank reconciliation records	6years	Delete Electronic Files/Shred hard copy files	Finance Manager
Monthly governing body financial reports	6 years	Delete Electronic Files/Shred hard copy files	Finance Manager
Minutes of meetings relevant to the Finance office and other staff members	6years	Delete Electronic Files/Shred hard copy files	Finance Manager
Financial reports for student assistance and disability reports	6years	Delete Electronic Files/Shred hard copy files	Finance Manager
Copies of financial procedures	Indefinitely		Finance Manager

IT

Document/record	Retention period	Action	Responsible
Software Licence	Indefinitely		IT Manager
Network account usernames - students	1 year after the individual has left the College		IT Manager
Network account usernames - staff	Duration of employment - Security copies for a further 3 months.		IT Manager

Marketing

Document/record	Retention period	Action	Responsible
General minutes of meeting	Indefinitely		Marketing Manager

Prospectus, student handbooks, graduation booklets, marketing literature	Indefinitely		Marketing Manager

Data Protection

Document/record	Retention period	Action	Responsible
Data Protection Requests and all materials pertinent to each request	5 years		Information Security Committee
Request Register	Indefinitely		Information Security Committee

1.8 Document Control

Document Title	Data Retention Schedule
Author	Data Protection Representative
Version	4.0
Date created	July 2021
Review	June 2022

1.9 Data Deletion

Data destruction is a critical component of a data retention policy. Data destruction ensures that the College will use data efficiently thereby making data management and data retrieval more efficient and cost effective. When the retention timeframe expires, the College must actively destroy the data covered by this policy. If a user feels that certain data should not be destroyed, he or she should identify the data to his or her supervisor so that an exception to the policy can be considered. Since this decision has long-term legal implications, exceptions will be approved only by a member or members of the College management team.

The College specifically directs users **not to** destroy data in violation of this policy. Destroying data that a user may feel is harmful to himself or herself is particularly forbidden or destroying data in an attempt to cover up a violation of law or company policy.

Data will be held across a number of databases depending on the subject's status. On audit and review of data in line with deletion policy the College will remove subject personal data on a permanent basis.

In accordance with GDPR guidelines a Data Subject can request to have their data removed on a permanent basis from our database. Where an individual contacts the College in this regard, we have specific steps that we follow to ensure the request is actioned in the most appropriate and effective manner.

- Data Controller i.e. the College have 28 days to action and complete request (*in accordance with GDPR guidelines).*
- Data Protection Representative to Speak to the Data Subject directly to confirm their request and outline the process including our statutory obligations to report to Springboard where applicable and advise we have 28 days to complete the request.
- Get Data Subject to complete the Data Deletion request form.
- Data Protection Representative to contact owners of various databases and filing systems in the College to sweep the database/hardcopy files for all data subject information and remove permanently in a secure manner.
- The data base owner on completion of this task reports back to Data Protection Representative to confirm all information removed.
- Final contact with data subject from Data Protection Representative to confirm all records are deleted.
- All appropriate records relating to this request to be save in the GDPR folder.

1.10 Data Protection Breach

1.10.1 Overview Data Breach Policy

The GDPR (*General Data Protection Regulation*) defines a 'personal data breach' as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

1.10.2 The College's Data Breach Policy:

Prevention is better than cure and all the College staff have been trained and understand GDPR policy and the importance at all times of protecting all information we hold in respect to a data subject.

In accordance with the GDPR guidelines the College employees shall not disclose any Data Subject's Information (including Personal Data), unless our Policies allow such disclosures.

Regardless of the measures that are taken in accordance with the above paragraph and related policies, there is always a risk of data security incidents arising. Data security incidents may range from relatively minor incidents, which do not actually result in unauthorised disclosure, loss, destruction or alteration of personal data, to major security incidents, such as the loss or theft of devices, such as laptops, which contain personal data.

The College Staff must report all suspected data security incidents to the Data Protection Response Team, Incidents include:

- Disclosure, loss, destruction or alteration of Customer Confidential Information, regardless of whether it is in paper or electronic form.
- The Data Protection Response Team will consider whether the incident constitutes a personal data breach. If the incident does constitute a personal data breach, the Data Protection Response Team will consider whether a notification to DPC is required.
- The Data Protection Response Team will also take such steps as are required to stop, contain or mitigate the effects of the data security incident and ensure that appropriate steps are taken in response to the incident, including the putting in place of new policies and procedures where necessary.
- Where a personal data breach occurs, it must be reported to the Data Protection Commissioner and other stakeholders without delay and, where feasible, not later than 72 hours after the College become aware of the breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.
- Where a personal data breach is likely to result in a high risk to the rights and freedoms of affected data subjects, then those data subjects must also be notified without undue delay.
- When assessing whether there is a high risk to data subjects it is important to bear in mind that one of the core purposes for notifying data subjects is to help data subjects take steps to protect themselves from any negative consequences of the breach.
- Notifications to the Data Protection Commission must include the following information:
    a) a description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned
    b) approximate number of personal data records concerned.
    c) the name and contact details of the Data Protection Response Team.
    d) a description of the likely consequences of the personal data breach; and
    e) a description of the measures taken or proposed to be taken by the College to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
    f) Notifications to data subjects must include the information set out above.

The College will also ensure that an appropriate record of the data security incident as well as any associated communications, are maintained in a Data Security Incident Log. The record should at a minimum include a brief description of the nature of the data security incident as well as whether the incident was reported.

Any notifications to affected data subjects or the Data Protection Commission will be made by an appointed individual from the College Data Protection Response team. Individual staff members should not make any such communication.

1.11 Data Backup and Recovery

Information security is extremely important to the College, driven in part by GDPR and advances in technology. Information security ensures that the College data and infrastructure are protected from

risks such as unauthorised access, destruction or loss of data, as well as unauthorised disclosure or incorrect processing of data.

1.11.1 Purpose of data backup and recovery

The primary objective of the policy is to protect the College data from loss and ensure it can be recovered in the event of equipment failure, a destruction or becoming inaccessible. This policy seeks to outline the data backup and recovery controls for the College employees to ensure that the data is correctly and efficiently backed up and recoverable in line with best practice.

1.11.2 Scope of data backup and recovery

This Data Backup and Recovery Policy has been created to guide and assist the College to align with GDPR, regarding data backup, recovery controls and procedures.

The policy applies to all employees of the College. This policy is crucial to the effective protection of data and a means for its recovery.

This policy applies to company related data that is stored locally by users on desktops, laptops, tablets and mobile phones. This includes both Windows, Mac and Android devices all of which are compatible with Microsoft OneDrive.

This policy does not relate to corporate email or contacts which are automatically synchronized with the user's device and the College Microsoft Exchange Server.

This policy does not relate to applications managed by the College Services that store, process or transmit information, including network and computer hardware, servers, or software and applications either locally or cloud hosted.

1.11.3 Policy

11.12.1.1 What cloud storage services can I use to store and share information at the College?

For the purposes of work-related file storage or file sharing, employees at the College may use either OneDrive or SharePoint service that is associated with their College Microsoft Office365 account.

- Employees should take care to ensure that they do not use a OneDrive account (such as a personal Microsoft account) that is not associated with their College Microsoft Office365 account to store or share work related files.
- Employees who have been using alternate cloud platforms for work related file storage or file sharing should immediately discontinue this practise. This includes services like Google Drive, Drop box, iCloud etc. These are not corporately supported services by the College.
- OneDrive or SharePoint offer equivalent functionality to alternate cloud platforms. If you are migrating from using an alternate cloud services please seek technical assistance if you have difficulty replicating features, functionality or processes in OneDrive/SharePoint.
- Continued use of alternate cloud platforms for work related file storage or file sharing by an employee will place them in breach of the College GDPR compliance policies.

It is the responsibility of the individual to ensure that their device is correctly synchronised with their corporate OneDrive and that they use and manage OneDrive in a way that synchronises work related

data that is created on their local device. The College IT Services have issued guidelines on how to configure OneDrive on your device; however, please request support directly if you require assistance in setting this up.

OneDrive provides powerful functionality for users who need to recover working versions of files or folders that are missing, deleted or corrupted. Users may please request assistance from the College IT services if needed for such data recovery.

1.11.3.1 Why will the College not permit the use of alternate cloud platforms?

It is impractical for the College at a corporate level to support alternate cloud platforms while at the same time maintaining a high degree of GDPR compliance. The terms of use, privacy policies and other user obligations of such services, would need to be reviewed and approved for use, on an ongoing basis are they are updated by the College. The proliferation of accounts, their management and security could not easily be managed as they are not synced with the College Microsoft Office365 accounts. It would be impractical for the College to have a robust process to respond to data requests, right to be forgotten requests or data breech incidents.

1.11.4 Removable Media Policy

Removable media is a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organisations. Employees should take care to limit the circumstances in which the make use of removable media to minimise the risk of loss or exposure of sensitive information and to reduce the risk of acquiring malware infections.

When using removable media suitable encryption software should be used to secure the drive.

Sensitive information including that of Personal Data as defined under GDPR should not be stored on removable media.

Removable media should not be used as a form of data backup and recovery. Employees should use OneDrive for this purpose.

Exceptions to this policy may be requested on a case-by-case basis. Such requests should be made to the IT Manager.