

# National College of Ireland

## Quality Assurance Handbook



9. Information Governance and Compliance  
November 2018

9.	Information Governance and Compliance.....	9-1
9.1.	Policy on information systems & Governance .....	9-1
9.2.	Data .....	9-1
9.3.	Training .....	9-2
9.4.	Key Performance Indicators .....	9-2
9.5.	Records Management Policy .....	9-3
9.6.	Data Protection Policy .....	9-6
9.7.	Personal Data Breach Handling.....	9-24
9.8.	Appendix 9-1: NCI Key Performance Indicators .....	9-26
9.9.	Appendix 9-2: Data Retention Schedules .....	9-41
9.10.	Appendix 9-3: NCI Privacy Statement.....	9-42

## 9.1. POLICY ON INFORMATION SYSTEMS & GOVERNANCE

National College of Ireland (NCI) is committed to having information systems that support teaching and learning, the implementation of quality assurance policies and procedures, and effective and efficient decision making. Information systems are selected and implemented in consultation with the wider user community using the NCI's **procurement process**, a project management approach and are required to adhere to the principles of privacy by default and accessibility by design.

NCI's information systems are centrally procured and managed by the IT department. Enterprise systems are procured on the basis that they are supported by a reputable vendor with sufficient support available to NCI. Where systems are cloud based, data must be held in the EU and the vendor must engage with NCI's data protection and information security policies

This overarching policy statement is supported by key individual policies as outlined below.

## 9.2. DATA

In order to maintain good governance of data, data will be held only once where feasible. Procedures are in place to share common data effectively and efficiently across systems. Procedures are in place to ensure that data is recorded accurately and to assure the security of that data. Figure 9.1 below is a graphic representation of the relationship between systems. The green-coded systems are those that are 'origin' or 'single source of truth' systems for course, module, staff and student biographical and curriculum data. Data originating from these must be updated/corrected at source.

Table 9-1: Table of Critical Information Systems

System	Area of Management
Core HR	Staff and External Examiners
Akari Document	Programme and module validation
QuercusPlus	Student Record System (Admissions, Records, Assessment, Awards)
Microsoft Dynamics	Students – Disability Support; Work placement; Careers services; Application for extenuating circumstance; applications for feedback
	External Stakeholder records
Moodle	Learning management system
Platform Avenue	Portfolio management
CAPITA	Library management system
Pharos	Print management system
CCure	Student Badge – Access Control
Syllabus Plus	Timetabling
TDS	Attendance Monitoring
Office 365	Credential authorisation
Evasys Survey	Learner and other stakeholder feedback

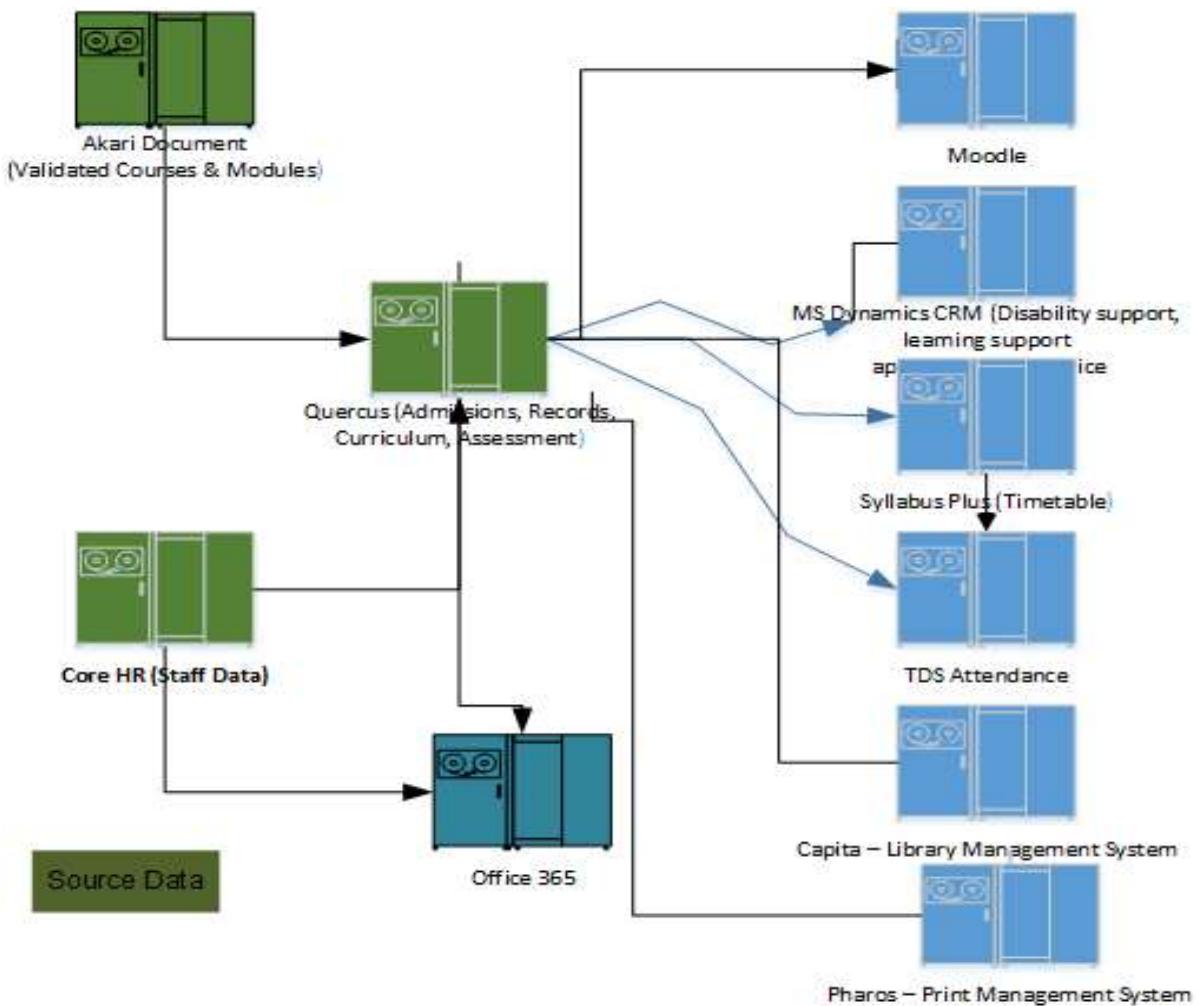


Figure 1: Information System Relationships

### 9.3. TRAINING

Staff will be trained on information systems prior to their use. This training may be delivered face-to-face, through the distribution of user manuals or by blended or online learning. Procedures are in place for this training to be monitored via the staff induction and probationary period.

### 9.4. KEY PERFORMANCE INDICATORS

As part of its internal and external reporting mechanisms, NCI uses a number of indicators as measures or as proxy measures for performance of learners, programmes and the institution. In creating these indicators, NCI has paid regard to national and international definitions for the calculation of measures, such as the Higher Education Authority (HEA), Quality and Qualifications Ireland (QQI), U-Multirank and Australian Tertiary Education Quality and Standards Agency (TEQSA).

Indicators may be presented at institutional, School, programme or modular level. These indicators are used to highlight areas of good practice and also areas of risk. Indicators relating to programmes, students, and graduates are coded in alignment with the guidance provided by the HEA for its annual statistical returns. Indicators relating to staff and knowledge transfer are aligned to the measures published by HEA in its *Higher Education System Performance, Institutional and Sectoral Profiles* series.

Reports based on these indicators are considered at academic and executive governance committees and provided where relevant and programme level to programme committees.

NCI's Key Performance Indicators are included in Appendix 1.

## 9.5. RECORDS MANAGEMENT POLICY

National College of Ireland (NCI) is committed to achieving compliance with best practice and recognised international standards with regard to record keeping and records management. **The aim of National College of Ireland's records management procedures is the creation and maintenance of full and accurate records, reflecting the functions and activities of National College of Ireland.**

### 9.5.1 Purpose

The purpose of this policy is to **provide a clear statement of NCI's commitment to effective records management as part of its overall efforts to ensure good governance, efficiency, accountability and compliance. It is also intended to set out the overall records management strategy by identifying some of the major elements of NCI's records management programme and mandating the development and implementation of these and other elements.**

The policy also recommends the establishment of suitable structures within NCI in order to facilitate the successful implementation of the records management programme; identifies the roles and responsibilities of NCI staff and management with regard to records management; and ensures the preservation of records of permanent value and establish archival criteria to maintain continued access to appropriate historical records.

### 9.5.2 Scope

All information created or received by NCI staff (including faculty and support staff, permanent and non-permanent), contractors, consultants and other agents in the course of their duties on behalf of NCI, preserved in the form of records, is covered by this policy statement. For **the purpose of this policy, the definition of 'record' in ISO 15489 applies**, "information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business".

This policy applies to all NCI records, regardless of format or location. For the purpose of this policy, locations as defined in the Freedom of Information Act 2014 will apply:

- (a) a book or other written or printed material in any form (including in any electronic device or in machine readable form); (b) a map, plan or drawing; (c) a disc, tape or other mechanical or electronic device in which data other than visual images are embodied so as to be capable, with or without the aid of some other mechanical or electronic equipment, of being reproduced from the disc, tape or other device; (d) a film, disc, tape or other mechanical or electronic device in which visual images are embodied so as to be capable, with or without the aid of some other mechanical or electronic equipment, of being reproduced from the film, disc, tape or other device, and (e) a copy or part of any thing which falls within paragraph (a), (b), (c) or (d).

This statement is applicable to all parts of the NCI organisation and includes all departments, offices, units, and areas of work which **form part of the organisation's structure**. It does not apply to non-records, which are defined as those used and kept for reference only, or personal documents which were not created or received in the transaction of NCI business.

Examples of non-records include: unsolicited advertising/promotional material; product brochures/catalogues; unsolicited emails; trade publications by companies or public bodies; personal emails (not relating to NCI activities). See the Records Management Procedural Manual for further details and guidance.

---

### 9.5.3 Ownership of records

All records created in the course of its official business constitute the official records of NCI. All records, irrespective of format (i.e. both textual and electronic) created or received by NCI staff or agents carrying out activities related to the business of NCI, are the property of NCI and subject to its overall control. Employees leaving NCI or changing positions with the organisation must leave all records available for their successors.

---

### 9.5.4 Structures and Responsibilities

The Director of Quality Assurance & Statistical Services (DQASS) will have overall responsibility for coordinating the implementation of this Records Management Policy.

The DQASS will convene a Records Management Group (RMG) in order to ensure that this policy and all associated procedures and guidelines are disseminated and implemented throughout NCI. The role of the RMG is to:

- Develop and approve policy for the creation, management and disposition of records
- Agree procedures for the creation, management and disposition of records
- Ensure that appropriate resources exist to support the policy and procedures and that all staff members are aware of the policy and comply with it.

Specific duties of the RMG include:

- Ensuring that appropriate structures are in place to facilitate the successful implementation of the Records Management Policy and all associated guidelines and procedures; this may involve, where necessary, delegating specific tasks or responsibilities to relevant managers or staff members.
- Ensuring that appropriate resources are allocated in order to achieve successful implementation of and compliance with the Records Management Policy and all associated guidelines and procedures.
- Establishing procedures for facilitating awareness of records management amongst staff.
- Establishing procedures to ensure ongoing review and updating of the Records Management Policy in order to ensure continuing compliance with legislative and regulatory requirements.

Membership of the RMG will be occasionally reviewed.

---

### 9.5.5 Systems and Responsibility

NCI is committed to the use of trustworthy record-keeping systems and procedures which ensure the integrity and authenticity of records captured, maintained and retrieved. Such systems and procedures aim to:

1. ensure that adequate records of business activities are being created and maintained, and that these records are authentic and reliable;
2. ensure that appropriate access controls are in place to safeguard confidential or sensitive records;
3. enable records to be arranged effectively to facilitate efficient retrieval;
4. ensure that records required for legal, administrative and fiscal purposes are retained for as long as they are needed;
5. ensure that records no longer required are destroyed according to the agreed retention policy;
6. identify and protect vital records essential for the operations of NCI;
7. ensure that adequate storage is provided for the records in a safe and secure environment.

Record-keeping systems will be designed and implemented in the overall context of NCI's ICT strategies and policies. The implementation of the Records Management Policy will be facilitated by the development of a set of detailed procedures and guidelines which will be put into operation by National College of Ireland. These will include:

- Staff Records Management Manual, with detailed instructions and procedures for the naming, saving, maintenance and overall control of records within the organisation.
- Records Classification Scheme, to aid the consistent classification and registration of records within NCI, and the efficient retrieval of records by authorised officers of the NCI.
- Records Retention Schedule, to identify suitable retention periods for all records generated in the course of the business activities of NCI, to ensure compliance with legal minimum retention requirements, and to ensure the disposal of records in a controlled and managed manner.
- Such other procedures, guidelines or policies as NCI considers appropriate in the context of implementing effective records management within the organisation.

### **9.5.6 Responsibilities**

It is the responsibility of the Governing Body and the senior executives to endorse records management policies and strategies and to ensure that the necessary management support is in place in order to facilitate implementation.

Each Head of School/Function/Department is required to ensure that the appropriate structures and resources are in place at the local level in order to ensure awareness of and compliance with this policy and the various procedures and guidelines that stem from it. Each School/Function/Department will have a Designated Records Officer, with responsibility for implementing this policy and the various procedures and guidelines within their respective team, and for providing feedback and comments as part of the review and ongoing monitoring process.

All staff, at every level, have a responsibility to observe and implement records management procedures, according to NCI policies and guidelines. This includes a requirement to be aware of and familiar with this policy and all associated procedures and guidelines. NCI recognises that the responsibility for the success of the records management programme is dependent on the commitment of all staff, including senior management and all permanent, temporary, part-time and contract staff.

## **9.6. DATA PROTECTION POLICY**

In line with data protection requirements and good practice, NCI wish to put in place, and be able to demonstrate, appropriate and effective management of personal data throughout the organisation.

NCI wishes to demonstrate commitment and compliance with the current Data Protection Acts and the General Data Protection Regulation (GDPR). Fundamental to the GDPR is the principle of accountability. Controllers and processors are both responsible and accountable for the protection of personal data, and must be able to demonstrate how they maintain compliance with data protection requirements.

**The implementation of an approved Data Protection Policy goes towards demonstrating NCI's commitment to the protection of personal data, and provides a basis for maintaining and improving compliance with data protection requirements and good practice.**

---

### **9.6.1 Purpose**

NCI collects, processes, and stores significant volumes of personal data and sensitive personal data (special category data) on an ongoing basis. The purpose of this document is to provide a statement of intentions for managing compliance with data protection requirements which is formally approved by senior management. This policy and the associated procedures, therefore, will ensure that everyone handling personal data is fully aware of the requirements and capable of acting in accordance with data protection procedures.

The objectives of the data protection policy are to:

1. Enable NCI to meet its own requirements for the management of personal data.
2. Ensure NCI meets applicable statutory, regulatory, contractual and/or professional duties.
3. Protect the interests of individuals and other key stakeholders.
4. Support organisational objectives and obligations.
5. Impose controls in line with NCI acceptable level of risk.

---

### **9.6.2 Scope and Constraints**

This policy applies to all personal data processed by NCI, regardless of the media on which the personal data is stored, i.e. paper-based, electronic, CCTV, etc.

This policy applies to:

- any person who is employed by NCI or is engaged by NCI, whether on a paid or voluntary basis, including contractor and sub-contractors, and who processes personal data in the course of their employment or engagement.
- any student of NCI who processes personal data in the course of their studies for administrative, research and/or any other purpose.

Failure of any staff member or agent to comply with this policy may lead to disciplinary action being taken in accordance with NCI's disciplinary procedures. Failure of a third party

contractor/subcontractor to comply with this policy may lead to termination of the contract and/or legal action.

---

### **9.6.3 Policy Review, Approval, and Continuous Improvement**

In line with best practice, this policy has been approved by senior management, along with a commitment of continual improvement. This document will be reviewed at least annually by senior management and the NCI Data Protection Officer to ensure alignment to appropriate risk management requirements and its continued relevance to current and planned operations, legal developments, legislative obligations, and information commissioner guidance.

---

### **9.6.4 Related Documents**

- [General Data Protection Regulation](#)
- [Data Protection Bill \(2018\)](#)
- [Working Party 29 Guidance on the Concepts of 'Controller' and 'Processor' \(2010\)](#)

This document forms part of NCI's Personal Data Management System, and should be read in conjunction with the other documents within the management system:

- NCI Data Protection Policy
  - NCI Data Retention Schedules (see Appendix 9-2)
  - NCI Privacy Statement (see Appendix 9-3)
- 

### **9.6.5 Definitions**

The following key GDPR terms and definitions are provided here for ease of use. For a complete list of definitions refer directly to the regulation in Section 9.6.4 above.

#### ***9.6.5.1 Anonymisation***

The process of turning data into a form which does not identify individuals and where identification is not likely to take place. This allows for a much wider use of the information.

#### ***9.6.5.2 Personal Data***

**'Personal data'** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, 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.

Recital 26 clarifies the issue of anonymous information, explaining that:

the principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to Personal Data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not, therefore, concern the processing of such anonymous information, including for statistical or research purposes.

#### ***9.6.5.3 Special Categories of Personal Data***

These refer to the processing of Personal Data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

NCI will avoid all processing of special categories of personal data where possible. It is understood that certain business activities within NCI require the processing of special categories of data (e.g. processing of data concerning health and disability). The general processing of special categories is prohibited in NCI, and in the rare instance it is required, Head of Departments must ensure all processing is defined in the data inventory, along with an appropriate legal basis (reference 1, Art 6), and derogation (reference 1, Art 9) for processing of such special categories recorded within the data inventory.

#### ***9.6.5.4 Data Controller***

The data controller refers to the natural or legal person, public authority, agency or another body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

In certain instances, NCI alone determines the purpose and means of processing, and in other instances, NCI might jointly determine the purpose and means of processing with a third party. In both circumstances, NCI would be considered a controller of this information. Section 9.6.5 above of this policy provides further information on the responsibilities of controllers, processors, and third parties.

#### ***9.6.5.5 Data Subject***

The data subject is any living individual who is the subject of personal data held by an organisation. Data subjects within NCI may include members of the public, students (current, past, and prospective), employees (current, past, and prospective), suppliers (e.g. sole traders or staff acting on behalf of the supplier), and other individuals such as external third parties, CPD members, and any other individual NCI might communicate with.

#### ***9.6.5.6 Processing***

This refers to any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use,

disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

#### **9.6.5.7 Processor**

The processor is a natural or legal person, public authority, agency or another body which processes personal data on behalf of the controller.

#### **9.6.5.8 Pseudonymisation**

This refers to the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

Examples of pseudonymisation within NCI may include the use of student IDs instead of student names for access authorisation. Where anonymisation cannot be used, the next best means of pseudonymisation should be used.

#### **9.6.5.9 Recipient**

This term refers to a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

---

### **9.6.6 Roles and Responsibilities**

**Everyone is responsible to ensure compliance with NCI's data protection requirements and obligations.** It is the responsibility of all staff to ensure:

1. They familiarise themselves with this policy and handle personal data in accordance with this policy, the data protection principles, and data handling rules.
2. They complete the mandatory data protection training provided. Data Protection training is mandatory for all NCI employees. Annually, all NCI staff will have to complete this training and a record maintained for audit purposes.
3. Queries in relation to personal data are promptly and courteously dealt with. When an employee receives an enquiry about the handling of personal data, they must know what to do, and/or where to refer it.

To ensure all users are aware of their responsibilities as users of NCI systems, the following sections include additional requirements based on key data protection roles within NCI. While all staff and agents of NCI have a responsibility to ensure Data Protection compliance, the following sections include additional requirements for key, specific data protection roles within NCI.

---

## **9.6.7 Governing Body and Senior Management**

The governing body and senior management are responsible for approving and reviewing this policy, and for mandating the allocation of appropriate resources to ensure its successful implementation. Each member of the Governing Body and Executive is responsible for ensuring compliance with the Data Protection Acts and GDPR in their respective areas of responsibility.

### **9.6.7.1 *Data Protection Officer***

As NCI is a public body, it is mandatory that a suitably trained, independent, senior role of Data Protection Officer (DPO) is appointed. This may be performed as a team function **provided a single individual is the lead person “in-charge” and roles within the DPO Team** team are clearly defined.

The responsibility of the DPO function within NCI is to:

1. Respond to individuals (data subjects) whose data is processed on all issues related to the processing of their data and the exercise of their data protection rights.
2. **Cooperate with the supervisory authority, and act as the organisation's contact point** for the supervisory authority on all issues related to the processing of Personal data in NCI.
3. Inform and advise NCI and its employees of their obligations pursuant to privacy regulations.
4. Monitor compliance with the data privacy obligations in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising, and training of staff involved in processing operations and the related audits.
5. To provide advice and assistance regarding the requirement to perform Data Protection Impact Assessments, and monitor their performance.
6. Arrange at least annual data protection training sessions.
7. Maintain a log of all data breaches and communication of breaches to all relevant parties when required to do so (supervisory authority, controllers, and data subjects).

Please refer to Section 9.7 below for more details.

To allow for the effective performance of their tasks, NCI will ensure:

1. The DPO will be suitably trained and have expert knowledge of Data Protection Law.
2. NCI will support the DPO in performing the tasks above by providing resources necessary to carry out those tasks. The key to this is to provide sufficient time, finance, and staff where appropriate to fulfil the DPO duties.
3. No tasks and duties result in a conflict of interests for the DPO.
4. That the DPO is involved, properly and in a timely manner, in all issues which relate to the protection of personal data, and will be in a position to perform their duties and tasks in an independent manner. Specifically:
  - a. The DPO will report directly to the NCI Board.
  - b. The involvement of the DPO will be sought where decisions with data protection implications are taken. All relevant information must be passed on to the DPO in a timely manner in order to allow him or her to provide adequate advice.
  - c. The DPO will participate regularly in meetings with senior and middle management.
  - d. The opinion of the DPO will always be given due weight.

- e. The DPO must be consulted without delay in the event of a data breach or other data protection incident occurring.
- 

#### 9.6.8 Human Resources

NCI Human Resources personnel have a key role in the management and protection of personal data which includes responsibility for:

1. Ensuring all new members of staff are made aware of this policy document at induction stage and that it is referenced in staff Terms and Conditions, Contracts, and Role Descriptions.
  2. Ensuring new starters and temporary staff who require training complete the first available data protection training course after their start date.
  3. Handling all employee-related personal data in accordance with this policy, the data protection principles, and data handling rules.
- 

#### 9.6.9 Head of Functions and Departments, Business Owners and Line Managers

Line Managers and Heads of Functions or Departments have a key role in the management and protection of personal data which includes responsibility for:

1. Ensuring all processing within their department is in compliance with the NCI Data Protection Policy and privacy best practice. Specifically, maintaining the data inventory of all information processed by their department, and for ensuring that staff in their area are aware of the policy, and the general obligations and requirements of data protection.
2. Ensuring their reporting staff complete the mandatory data protection training.
3. Ensuring sufficient resources are available to support the effective implementation of this policy.
4. Ensuring appropriate technical and organisational security measures, including anonymisation for statistical and research purposes, are in place in areas for which they are responsible. Specifically, security risk assessments will be undertaken to check that the personal data is sufficiently protected in line with security policy. Security risk assessments will be commissioned regularly and evidence retained for audit purposes. To deal with appropriate technical and organisational security measures, the line manager/head of function may delegate the security tasks, in full or partially, to another NCI representative. This delegation does not exempt the line manager/head of function from their responsibility and they must make sure that the delegated jobs have been carried out correctly.
5. Ensuring data privacy risks are appropriately managed within their function. Specifically, to ensure the handling of personal data is regularly assessed and evaluated. Under the GDPR there are a number of changes which will affect both in-house changes and contracts for new projects. It is therefore important that if any new projects are being considered then data protection needs to be built in at the beginning (Privacy by Design and Default), and contracts will need to reflect the necessary changes.
6. Ensuring that where processing “**is likely to result in a high risk to the rights and freedoms of natural persons**” and/or “**processing on a large scale of special categories of data**”, a **Data Protection Impact Assessment** is formally carried out in relation to each new project or proposal (see Section 9.6.21 below for more details on Data

Protection Impact Assessment). The NCI DPO must be informed and involved at an early stage.

7. Ensuring regular consultation with the DPO, and facilitating the DPO in performing their compliance audits.

---

#### **9.6.10 Technical Solutions Architects / Technical Design Leads / Project Managers**

Members of staff and other third parties involved in the planning, design, build, and change of technical solutions have a key role in the protection of personal data which includes:

1. Ensuring the protection of personal data is considered for all changes and managed projects within NCI.
2. Where changes and projects do not include the collection and processing of personal data, this must still be documented and signed off by the Project Manager, and retained as evidence for audit purposes.
3. Implementing the principles of data protection by design and data protection by default, and retaining evidence of this for audit purpose as part of the Project Management Lifecycle (see Section 9.6.19 below for more details).

---

#### **9.6.11 Compliance with the Data Protection Principles**

NCI is committed to ensuring all personal data is processed in line with the General Data Protection principles and good practices.

##### **9.6.11.1 *Lawfulness, Fairness and Transparency***

***Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.***

NCI is committed to ensuring the lawful, fair, and transparent collection of data. Our data inventory records all information processed, including the lawful basis of such processing. In addition, our privacy notice provides all necessary information to data subjects about the processing of their data. The information is given in a concise, transparent, intelligible, and easily accessible form, and includes the purposes of processing, the period of processing, their rights, and the lawful basis for the processing. These privacy notices must be provided to data subjects prior to collecting personal data regardless of the collection method (phone, CCTV, forms, interview, website etc.).

##### **9.6.11.2 *Consent***

Where the lawful basis of processing is based on consent, NCI shall incorporate procedures for the obtaining and withdrawal of consent. Where consent is withdrawn, processing based on consent must cease. Specifically, where other departmental requirements or legislation require explicit consent (e.g. for marketing), the departments shall contain procedures for collecting this consent. The department must also monitor all requests for removal or withdrawals of consent, maintain a register of all such requests, and ensure that all removals are completed without undue delay.

Where processing on the lawful basis of consent, and the processing relates to a child (reference 2 – this is 13 years of age), the department must ensure they have obtained and recorded consent provided by the holder of parental responsibility for the child. The DPO for further guidance, clarification, and consultation in relation to the lawfulness of processing, and conditions for consent.

#### **9.6.11.3 Purpose Limitation**

***Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.***

NCI is committed to only collecting and processing information for an explicit purpose. All information processed, along with the business purpose, is detailed within the data inventory which will be reviewed and updated at least annually, or when any significant changes occur to the data processed, where it is processed, or with whom it is shared.

Personal data will only be processed for the defined purpose. All requests for changes to the use of personal data must be compatible with the original purpose for processing. If additional purposes are required, consent may be required to be sought from the data subject for this change of purpose.

#### **9.6.11.4 Data Minimisation**

***Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.***

NCI is committed to only collecting and processing appropriate information to the extent needed to fulfil the operational and service needs, and to comply with all applicable statutory, regulatory, contractual and/or professional duties. Data will be minimised, and the minimisation shall be enforced through Data Protection Impact Assessments (DPIAs), and Data Protection by Design and Default procedures within the change management/project management teams.

#### **9.6.11.5 Accuracy**

***Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.***

NCI is committed to taking all reasonable efforts to ensure the accuracy of the personal data. This will be planned for, and enforced, through DPIAs, and Data Protection by Design and Default procedures within our change management/project management teams.

#### **9.6.11.6 Storage Limitation**

***Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the Personal data are processed.***

NCI have documented the required data retention periods along with justification and action to be taken when the retention period expires. The Data Retention Policy outlines the retention

period for all personal data across NCI, and what will occur when the retention period expires. It applies to all personal data, regardless of the media on which it is stored (paper-based, electronic, CCTV or otherwise). This policy helps ensure that NCI is maintaining the personal data for an appropriate length of time, based on legal and business requirements and in line with the data protection ‘storage limitation’ principle. Everyone is responsible to ensure this policy is adhered to.

#### **9.6.11.7 Integrity and Confidentiality**

*Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.*

NCI is committed to protecting and not disclosing personal data, either within or outside of NCI, to any unauthorised recipient. Everyone is responsible to protect against the accidental loss, destruction or damage to personal data, regardless of the media on which it is stored (paper-based, electronic, CCTV or otherwise).

#### **9.6.11.8 Individual Rights**

All data subjects have a wide array of rights in relation to the personal data which NCI process on their behalf. The GDPR creates some new rights for individuals, and strengthens some of the rights that currently exist.

The GDPR introduces a new best practice recommendation that, where possible, organisations should be able to provide remote access to a secure self-service system which would provide the individual with direct access to his or her information (Recital 63). This will not be appropriate for all departments, but there are some areas in NCI where this may be feasible and should be implemented.

---

#### **9.6.12 Common Procedures to Exercise Individual Rights**

Any queries regarding data protection, or any requests for personal data, whether from the person themselves or from a third party, must be referred to the DPO. Any person wishing to exercise this right must apply in writing (or email) to the DPO.

The procedure is as follows:

1. All data access requests directed to NCI must be in writing (or email), to the DPO. On receipt of a query or access request by telephone, please ask the caller to put their request in writing (or email), and to address it to the NCI DPO.
2. The DPO will check the validity of the access request. The GDPR does not introduce an exemption for requests that relate to large amounts of data, however, all efforts will be made to try to narrow the search to provide the data subject with relevant and concise information and avoid a disproportionate effort. Where the request is considered excessive, unfounded, or information which the data subject already holds, consideration will be given as to the validity of the request.

3. The request must include sufficient identification and details for the DPO to satisfy themselves that sufficient material has been supplied to definitively identify the individual. If the DPO can demonstrate they are not in a position to identify the data subject, additional information will be requested as necessary to confirm the identity of the data subject and the request will not be enacted upon until such identification is provided to the DPO. Personal data should never be provided to a data subject that has not been identified, nor should personal data be provided to the parent or legal guardian of a data subject where that subject is 13 years or older.
- 

#### 9.6.13 Right to Access

Data subjects (including employees, students, other individuals and members of the general public that may have availed of NCI's services, or received communications or information from NCI) have the right to access personal data held about them (this includes factual information, expression of opinion, and the intentions of NCI in relation to them, irrespective of when the information was recorded).

1. Where the access request is relevant to a number of departments, the DPO will contact the relevant departments and request them, in writing, to conduct a search of all data held by them. Such searches will be conducted in accordance with guidance provided by the DPO, and all steps taken to locate and collate data will be noted and documented.
  2. Each department must redact all information not relevant or not in scope for release. Where the department is unsure of what is relevant they must consult with the DPO. However, the responsibility for redacting irrelevant information remains with each department.
  3. Once any required review and redaction are completed, the personal data that is recommended for disclosure/deletion will be forwarded to the DPO for consideration. Department responses must also include an analysis of the relevant exemptions being relied upon, a description of the purpose of processing, to whom the data may have been disclosed, and the source of the data.
  4. If personal data relating to other parties (other than the requesting data subject) is involved, the personal data of the other parties must not be disclosed without their consent. Alternatively, the other party personal data may be anonymised so as not to reveal their identity. If an opinion of other parties (other than the requesting data subject) is involved, their opinion may be disclosed unless it is an opinion which was given in confidence on the clear understanding that it would be treated as confidential.
  5. A final decision on disclosure/deletion of the requested information will be taken by the DPO, in conjunction with the head of the relevant department(s) and legal advice where required.
- 

#### 9.6.14 CCTV Footage

CCTV footage is personal data within the meaning of the Data Protection Acts. The following provides the **Irish Data Protection Commissioners position** with regard to access to CCTV footage made under Subject Access Requests (reference Case Study 13 of 2013 in <https://www.dataprotection.ie/docs/CASE-STUDIES-2013/1441.htm>):

1. Any person whose image is recorded on a CCTV system has a right to seek and be supplied with a copy of their own personal data from the footage.

2. When making an access request for CCTV footage, the requester should provide the data controller with a reasonable indication of the timeframe of the recording being sought - i.e. they should provide details of the approximate time and the specific date(s) on which their image was recorded. For example, it would not suffice for a requester to make a very general request saying that they want a copy of all CCTV footage held on them. Instead, it is necessary to specify that they are seeking a copy of all CCTV footage in relation to them which was recorded on a specific date between certain hours at a named location. Obviously, if the recording no longer exists on the date on which the data controller receives the access request, it will not be possible to get access to a copy. Requesters should be aware that CCTV footage is usually deleted within one month of being recorded.
3. For the data controller's part, the obligation in responding to the access request is to provide a copy of the requester's personal data. This normally involves providing a copy of the footage in video format. In circumstances where the footage is technically incapable of being copied to another device, or where the supply of a copy in video format is impracticable, it is acceptable to provide stills as an alternative. Where stills are supplied, it would be necessary to supply a still for every second of the recording in which the requester's image appears in order to comply with the obligation to supply a copy of all personal data held.
4. Where images of parties other than the requesting data subject appear on the CCTV footage, the onus lies on the data controller to pixelate or otherwise redact or darken out the images of those other parties before supplying a copy of the footage or stills from the footage to the requester. Alternatively, the data controller may seek the consent of those other parties whose images appear in the footage to release an unedited copy containing their images to the requester.
5. Where a data controller chooses to use technology to process personal data, such as a CCTV system to capture and record images of living individuals, they are obliged to shoulder the data protection obligations which the law places on them for such data processing. In the matter of access requests for CCTV footage, data controllers are obliged to comply fully with such requests. Claims by a data controller that they are unable to produce copies of footage or that stills cannot be produced from the footage are unacceptable excuses in the context of dealing with an access request. In short, where a data controller uses a CCTV system to process personal data, it takes on and is obliged to comply with all associated data protection obligations.

The following procedure refers to the **UK Information Commissioners Office** with regard to access to CCTV Footage made under Subject Access Requests:

When disclosing surveillance images of individuals, particularly when responding to subject access requests, you need to consider whether the identifying features of any of the other individuals in the image need to be obscured. In most cases the privacy intrusion to third party individuals will be minimal and obscuring images will not be required. However, consideration should be given to the nature and context of the footage.

For example, if footage from a camera that covers the entrance to a drug rehabilitation centre is held, then consider obscuring the images of people entering and leaving it as this could be considered sensitive personal data. This may involve an unfair intrusion into the privacy of the individuals whose information is captured and may cause unwarranted harm or distress. **On the other hand, footage of individual's entering and exiting a bookshop is far less likely to require obscuring.**

Following the above, a case-by-case assessment is required as to the context of the CCTV. The DPO can provide further information and/or clarification on the procedure for managing such data requests.

---

#### 9.6.15 Right to Rectification

Data subjects (including employees, students, other individuals and members of the general public that may have availed of NCI's services, or received communications or information from NCI) have the right to the rectification of any inaccurate personal data concerning him or her that is held by NCI. This applies if data is inaccurate or misleading to a matter of fact. This is not an absolute right, and restrictions apply. For example, it does not apply to witness statements or opinions of others such as assessors, etc. Refer the data subject to the DPO for **all requests under the “Right to Rectification”**.

In the case of backups, the right to rectification may not be practical or possible, and may therefore be exempt. This would depend on the backup types, and the DPO should be consulted if there is any uncertainty.

---

#### 9.6.16 Right to Erasure

Data subjects have the right to obtain from the controller the erasure of personal data concerning him or her where there is no longer a legal ground for processing of the information. This is not an absolute right, and restrictions apply. Refer the data subject to the DPO for **all requests under the “Right to Erasure”**.

In the case of backups, the right to erasure may not be practical or possible, and may therefore be exempt. This would depend on the backup types, and the DPO should be consulted if there is any uncertainty.

---

#### 9.6.17 Restrictions

There are restrictions, and in certain circumstances, it may be prudent for NCI not to adhere to certain individual rights. The DPO will consider each request on a case by case basis and it is likely that such restrictions would not apply to the complete data set and more likely to a restricted and very specific set of personal data. For example, NCI may not be permitted to apply a blanket exemption to the right of access to an entire **set of a student's data because some elements may be considered privileged**, such as an opinion given in confidence regarding the student.

If NCI wishes to withhold certain subject rights, this must be referred to the DPO, who may seek legal counsel. Restrictions on exercise of data subject rights are laid out in the Data Protection Bill (reference 2), and shall be considered carefully when performing data subject access requests.

It should be noted that the existence of proceedings between a data subject and the data controller, for any reason, does not preclude the data subject making a data subject access request under the Act, nor does it justify the data controller in refusing the request. For example, if a data subject access request is refused, a response clarification as to which exemption is being applied, including the specific restriction, must be cited.

---

### 9.6.18 Information and Cyber Security

GDPR requires NCI to implement technical and organisational measures to ensure an appropriate level of security. NCI must take into account the current state and availability of security technologies, the costs of implementation, the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. NCI must also ensure their processors also implement appropriate measures. Some examples of appropriate measures as mentioned in the Regulation are:

- a) the pseudonymisation and encryption of personal data;
- b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

NCI fulfil these obligations by a number of means, specifically:

1. Deployment of Data Protection by Design and by Default within our Project Management Lifecycle for all new systems/changes to processing (see Section 9.6.19 below).
2. Regular risk assessments/testing to assess and evaluate the effectiveness of technical and organisational measures on existing processing (see Section 9.6.20 below).
3. **Formalised Data Protection Impact Assessments (DPIAs) where processing “*is likely to result in a high risk to the rights and freedoms of natural persons*” and/or “*processing on a large scale of special categories of data*”** (see Section 9.6.21 below).

Records of all of the above activities will be forwarded to the NCI DPO and retained for audit purposes.

---

### 9.6.19 Data Protection by Design and Default

GDPR requires:

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only Personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of Personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default Personal

data are not made accessible without the individual's intervention to an indefinite number of natural persons

As part of the implementation of Data Protection by Design and Data Protection by Default principles, a data protection and security design review will be performed during the development stage, and as part of the project management of all projects. The following is a minimum checklist for the areas that will be examined as part of this review, and records of the examination of each area must be maintained for audit purposes:

1. Has the Data Inventory been updated with any new forms of processing including data categories processed, where it is processed, and with whom it is shared?
2. Has a valid lawful basis for this processing been defined within the Data Inventory?
3. Do any new forms of processing include a relevant data privacy notice with all required information as defined in the NCI Data Privacy Notice(s) policy (reference NCI-PDMS-04)?
4. Is the information collected for a specifically defined purpose?
5. Is only the required information collected, or is information collected which may be deemed excessive (i.e. is the personal data that is collected minimised)?
6. How is the personal data kept reasonably accurate and up-to-date?
7. How long is the personal data retained for, and does the retention period and destruction method comply with the NCI Data Retention Policy (reference NCI-PDMS-03)?
8. Is it necessary for NCI to be able to identify the individuals whose data is being processed, or could anonymisation be used?
9. Could pseudonymisation be enforced to protect the personal data, for example, could individuals making enquiries regarding courses be restricted to a reference number until such time as they submit an application?
10. Can the personal data be encrypted at rest and/or in transit, and if not, are other security measures in place to adequately address the risks associated with the processing activity?
11. How is the information protected against unlawful or accidental loss, destruction or damage?
12. How does the new form of processing allow for the implementation of individual rights, including the right to access, rectification, and erasure?
13. Is all processing within the EEA?
14. Has a technical penetration test or risk assessment been performed and remediation actions were taken?
15. Are appropriate access controls in place? Specifically:
  - a. Is physical or remote access needed to the office in order to access the personal data?
  - b. Is user access restricted on a need-to-know basis?
  - c. Is all user access audited and do is there an audit trail of all user access?
  - d. Is there a formal process for joiners/movers/leavers to facilitate user access management?
  - e. Are user access reviews performed which are signed-off by relevant business owners and recorded for audit purposes?
16. Are other relevant and appropriate technical and organisational security measures applied? Specifically:
  - a. Is a formalised patching policy applied and maintained?
  - b. Are reliable and recent backups in place, and are these tested regularly?

- c. Are all backups encrypted?
  - d. Are appropriate perimeter security controls applied?
  - e. Is appropriate anti-malware deployed?
  - f.
17. Can personal data which is shared externally for reporting purposes, or retained for analytics/statistics, be anonymised?

---

#### 9.6.20 Regular Risk Assessment

GDPR Requires that *a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.*

It is the responsibility of the Head of the Department to ensure appropriate technical and organisational security measures are in place in areas for which they are responsible. Specifically, regular security risk assessments must be commissioned to check that the personal data is sufficiently protected based on the level of risk. Security risk assessments will be conducted regularly, and a record maintained for audit purposes with the output from each area examined. At a minimum, the risk assessment must evaluate and record the technical and organisational measures identified in the previous Section 9.6.19 above. Heads of Department may commission other NCI resources to assist with risk assessments.

NCI will ensure that any risks to the privacy of data are assessed, and that measures that are implemented are appropriate to the risks of the processing on the systems used. To facilitate this, each data category name, data store, and recipient/s (or third parties) are assigned a risk level based on a defined set of criteria for each department's Personal Data Inventory.

---

#### 9.6.21 Data Protection Impact Assessment

GDPR requires that a formalised Data Protection Impact Assessment (DPIA) is performed where processing "*is likely to result in a high risk to the rights and freedoms of natural persons*" and/or "*processing on a large scale of special categories of data*".

A data protection impact assessment will be carried out by NCI prior to the processing of the personal data, paying particular attention to the likelihood and severity of the risk, taking into account the:

1. Nature
2. Scope
3. Context and purposes of the processing
4. The sources of the risk

At a minimum, the DPIA will contain:

1. A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller.
2. An assessment of the necessity and proportionality of the processing operations in relation to the purposes.
3. An assessment of the risks to the rights and freedoms of the data subjects.
4. The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned. (Note: the list provided for Data

Protection by Design and Default will also be completed for the Data Protection Impact Assessment)

5. Where appropriate, NCI will seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

It is the responsibility of NCI and its designated business owners, not the DPO, to carry out DPIAs as necessary. However, the DPO shall be consulted at each stage of the DPIA, and shall provide advice and guidance as follows:

- whether or not to carry out a DPIA
- what methodology to follow when carrying out a DPIA
- whether to carry out the DPIA in-house or whether to outsource it
- whether or not the DPIA has been correctly carried out and whether its conclusions are in compliance with the GDPR
- whether or not to go ahead with the processing following a review of the DPIA
- what safeguards to apply if processing does go ahead

All consultation with the DPO will be retained as evidence for audit purposes. Where the advice of the DPO is not taken, the Article 29 Data Protection Working Party: Guidelines on DPOs recommends that the reasons for not adhering to the advice of the DPO should be documented. NCI shall formally record these reasons in the DPIA documentation. Further external guidance in the performance of a DPIA is provided by the following resources:

- <https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>
- <https://www.oaic.gov.au/resources/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments.pdf>
- <https://www.oaic.gov.au/agencies-and-organisations/guides/pia-guide-qrt>
- <http://www.pdp.ie/training/practical-guide-to-impact-assessments-data-protection-ireland-journal.pdf>

---

#### 9.6.22 Third Country Transfers

All NCI personal data must remain within the European Economic Area (EEA). Where a business need requires the transfer or processing information outside of the EU, the NCI DPO shall be contacted for consultation.

Particular attention is required to the selection of processors when using online services, such as cloud services, for the processing of information as NCI must ensure all processing remains within the EU, i.e. online marketing surveys, etc.

---

#### 9.6.23 Data Sharing – Controllers and Processors

The Article 29 Data Protection Working Party of the European Commission has published a guidance document on the concepts of ‘**data controller**’ and ‘**data processor**’, see Section 9.6.4 above9.6.5 above.

‘Data controller’ means:

1. the natural or legal person, public authority, agency or other body which,
2. alone or jointly with others,

- determines the purposes and means of the processing of personal data;

The following provides 3 typical activities conducted by a data controller within NCI.

<b>Scenario</b>	<b>NCI</b>	<b>Third Party</b>
Processing of Student Personal Data	Controller	Processor (FEI)
Processing of personal data for the provision of college accommodation (TCAS)	Controller	Controller
Processing of Student Personal Data	Processor	Controller (HEA)

In most instances, NCI has been identified as the Data Controller. Where there is uncertainty regarding the designation of NCI as either controller, processor, or joint controller, the DPO can be consulted for clarification.

#### *9.6.23.1 Requirements when Using Data Processors*

Whenever NCI share personal data with a recipient outside of the organisation, the sharing of the information must be governed by a contract that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller. This applies to all forms of sharing of information with recipients. For example, engaging the services of an external solicitor is no different to engaging the services of any other service provider. For that reason, it is unlawful for NCI to pass any personal data to an external solicitor unless NCI have put a contract in place describing the nature and purpose of processing, in addition to other specific contractual requirements as detailed in this section, i.e. the data protection principles, subject rights retained, etc.

#### *9.6.23.2 Evaluation of Processors*

NCI must use only processors providing sufficient guarantees to implement, and be able to demonstrate, appropriate technical and organisational measures taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons.

#### *9.6.23.3 Responsibilities as Data Controller*

All processing agreements must be governed by a contract that is binding on the processor with regard to the controller and that sets out:

- subject-matter
- duration of the processing
- nature and purpose of the processing
- type of Personal data and categories of data subjects

That contract or other legal act shall stipulate, in particular, that the processor:

1. Processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.
2. Processes all personal data within the EU.
3. Ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
4. Shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk including as appropriate:
  - a. the pseudonymisation and encryption of personal data;
  - b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
  - c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
  - d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
  - e. the account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
5. Assist NCI by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights under data protection requirements and good practice.
6. Assists NCI in ensuring compliance with the data protection obligations taking into account the nature of processing and the information available to the processor.
7. At the choice of NCI, deletes or returns all the personal data to NCI after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data.
8. Makes available to NCI all information necessary to demonstrate compliance with our data protection obligations laid down in the GDPR and allow for and contribute to audits, including inspections, conducted by NCI or another auditor mandated by NCI.
9. The processor shall immediately inform the controller if, in its opinion, an instruction infringes any data protection regulations, acts or good practices.
10. Where a processor engages another processor for carrying out specific processing activities on behalf of NCI, the same data protection obligations as set out in the contract between NCI and the processor shall be imposed on that other processor by way of a contract, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet NCI requirements. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to NCI for the performance of that other processor's obligations.

The above identifies minimum handling requirements only. Additional controls may be put in place for certain personal data types if required in addition to the above.

## 9.7. PERSONAL DATA BREACH HANDLING

### 9.7.1 What is a Personal Data Breach?

A “personal data breach” means 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.

Example of typical data breaches are:

1. Loss or theft of data or equipment on which data is stored
2. Loss or theft of documents/folders
3. Unforeseen circumstances such as a flood or fire which destroys information
4. Inappropriate access controls allowing unauthorised use
5. A hacking/cyber attack
6. Obtaining information from the organisation by deception, misaddressing of e-mails, human error, etc.

The above examples include the accidental loss of personal data as statistics indicate that most breaches are internal in nature and due to non-malicious user behaviour (e.g. loss of unencrypted laptop or USB, paper files, etc.).

### 9.7.2 Staff Responsibilities

In order for NCI to be able to comply with the GDPR, it is essential that all incidents (including suspected incidents) which give rise to the risk of unauthorised disclosure, loss, destruction or alteration of personal data are reported without delay to the DPO. Where the DPO is unavailable, a secondary point of contact shall be identified, and the incident shall be reported in line with the agreed procedure. In the event of a suspected personal data breach happening, employees shall notify the DPO immediately. Employees shall not assume that the DPO is already aware of the suspected breach.

### 9.7.3 Managing a Personal Data Breach

GDPR requires that NCI **document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance.**

In the event of a suspected personal data breach, a summary of the personal data breach shall be recorded in the NCI Data Breach Log. Each summary shall contain the facts relating to the personal data breach, its effects, and the remedial action taken. The NCI Data Breach Log shall be maintained by the DPO. Within NCI, the DPO will assess the breach, and make a decision on the next steps to be taken.

### 9.7.4 Notification of Data Breach

#### 9.7.4.1 *Notification to Supervisory Authority*

After review of the breach by the DPO, if the data breach likely affects the rights and freedoms of a data subject, the DPO shall inform the Irish Data Protection Commissioner within an

elapsed time of 72 hours of NCI becoming aware of the breach. The details of the notification will include:

1. Description of the nature of the personal data breach including, where possible, the approximate number of data subjects concerned, the categories of data concerned, and the approximate volume of data records concerned.
2. Description of the likely consequences of the personal data breach.
3. Description of the measures taken, or proposed to be taken, by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

#### ***9.7.4.2 Notification to Data Subjects***

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, NCI shall communicate the personal data breach to the data subject without undue delay. The notification shall describe in clear and plain language the nature of the personal data breach and contain at least:

1. Name and contact details of the NCI DPO.
2. Description of the likely consequences of the personal data breach.
3. Description of the measures taken or proposed to be taken by NCI to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

#### ***9.7.4.3 Notification to Controllers***

Where NCI performs the role of data processor the DPO will notify all data controllers without undue delay after becoming aware of a personal data breach including:

1. Description of the nature of the personal data breach including, where possible, the approximate number of data subjects concerned, the categories of data concerned, and the approximate volume of data records concerned.
2. Description of the likely consequences of the personal data breach.
3. Description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

## **9.8. APPENDIX 9-1: NCI KEY PERFORMANCE INDICATORS**

As part of its internal and external benchmarking and reporting mechanisms, NCI uses a number of indicators as measures or as proxy measures for performance of learners, programmes or of the institution. In creating these indicators, NCI has paid regard to national<sup>1</sup> and international definitions for the calculation of measures. Indicators may be presented at institutional, School, programme or modular level. These indicators are used to highlight areas of good practice and also areas of risk.

Indicators relating to programmes, students, and graduates are coded in alignment with the guidance provided by the HEA for its annual statistical returns<sup>2</sup>.

Indicators relating to staff and knowledge transfer are aligned to the measures published by HEA in its *Higher Education System Performance, Institutional and Sectoral Profiles* series

### **9.8.1 Admission & Registration KPIs**

Indicator	Measure of/Proxy Measure	Definitions/Formula	Data Source
Applications	<ul style="list-style-type: none"><li>• Attractiveness of a programme and/or NCI</li><li>• Effectiveness of 2<sup>nd</sup> level school liaison strategy</li><li>• Effectiveness of FE articulation strategy</li><li>• Effectiveness of Domestic Postgraduate Strategy</li><li>• Effectiveness of International Marketing strategy</li></ul>	Number of applications to NCI programmes – direct and to CAO  CAO primary indicator is number of 1 <sup>st</sup> preferences to level 8 programmes	Quercus  CAO application data

<sup>1</sup> Higher Education Authority.; <https://www.umultirank.org/about/methodology/indicators/>; <https://www.teqsa.gov.au/latest-news/publications/risk-assessment-framework>

Indicator	Measure of/Proxy Measure	Definitions/Formula	Data Source
No Offers	<ul style="list-style-type: none"> <li>Effectiveness of programme information</li> <li>Appropriateness and communication of entry requirements</li> </ul>	No offers made to applicants. Status of application is AOC, AO	Quercus
No. Converted Applications	<ul style="list-style-type: none"> <li>Effectiveness of programme information</li> <li>Efficiency of admissions process</li> <li>Marketing &amp; Recruitment Strategy (Domestic &amp; International)</li> </ul>	Number of offers that have been accepted; status of application is APA	Quercus
No. students registered	<ul style="list-style-type: none"> <li>Comms. Strategy at different stages of application process</li> <li>Early indicator of students in financial difficulty</li> <li>Early indicator of student withdrawal</li> </ul>	<p>Number of students registered at official census dates. Status 'R' 1 November; 1<sup>st</sup> March Limitations: These census dates preclude programmes that commence and complete between 1 March and 1<sup>st</sup> November.</p>	Quercus/HEA return
No. students registered as a percentage of those eligible to register		$x = \frac{\text{No of Students at status 'R'}}{\text{No of students at status (P + R + PCAO)}}$	Quercus
No. withdrawals before the November census dates or March census dates	<ul style="list-style-type: none"> <li>Early indicator of course not suitable to student</li> <li>Effectiveness of Student Orientation Programme</li> <li>Quality of Programme Information</li> <li>Suitability of Entry Requirements</li> <li>Consistency between Programme Information and Programme Structure and/or Module Content</li> </ul>	<p>In year withdrawal rate is defined as</p> $x = \frac{\text{No of Students at status 'RW'}}{\text{No of students at status 'R'}}$ <p>where date of withdrawal is &lt; 1-NOV-YYYY</p>	Quercus

Indicator	Measure of/Proxy Measure	Definitions/Formula	Data Source
Reasons for withdrawal	<ul style="list-style-type: none"> <li>• Challenges facing students and required support services</li> <li>• Visibility and/or Availability of Student Support Services</li> <li>• Retention rates for different cohorts, i.e. full-time, part-time, under/postgraduate, professional development, domestic/international, etc.</li> </ul>	Reasons for withdrawal are provided by students when they formally withdraw.	Quercus
No. students transferring from a programme	<ul style="list-style-type: none"> <li>• Appeal of course being transferred from/to</li> <li>• Quality of programme information within the School</li> </ul>	$x = \frac{\text{No of Students at status 'TRANSFER'}}{\text{No of students at status (R)}}$	Quercus
No. students transferring into a programme	<ul style="list-style-type: none"> <li>• Consistency between programme information and programme structure and/or module content</li> <li>• USPs of different programmes within the School</li> </ul>	$x = \frac{\text{No of Students at status 'R' with a student code of 'TI'}}{\text{No of students at status (R)}}$	Quercus

### 9.8.2 Learning, Teaching & Assessment KPIs

Indicator	Measure of/Proxy Measure	Definitions/Formula	Data Source
Disciplinary mix	<ul style="list-style-type: none"> <li>• Reliance on a subject and/or programme</li> </ul>	No of programmes by ISCED code No of students by ISCED code	Quercus
No. & percentage of students		$x = \frac{\text{No of Students at status 'R' with a student code of 'NE' in Academic Year - 1}}{\text{No of students at status 'R' with student code of 'RE' in Academic Year}}$	Quercus

Indicator	Measure of/Proxy Measure	Definitions/Formula	Data Source
progressing to the next stage of the programme	<ul style="list-style-type: none"> <li>• Student attainment v. MIPLOs</li> <li>• Parity between MIPLOs and MIMLOs</li> <li>• Quality of Teaching and Learning Modes</li> <li>• Effectiveness of Assessment Strategy</li> <li>• Suitable Workload</li> <li>• Student Engagement (Academic)</li> </ul>	<p>In calculating the progression of a cohort of learners, it is important that the initial cohort is isolated. To calculate the progression from stage 1 to stage 2, new entrants can be isolated by using the student code from the student hea record – <b>NE – new entrant</b>. When these students progress to the next stage of their programme, this value changes to '<b>RE</b>' – <b>re-enrol</b>.</p> <p>If stage 2 allows transfers from other programme or colleges, these students are discounted from the total number enrolled as to include them could mask a non-progression rate from stage 1.</p> <p>Progression in subsequent stages is calculated on the basis of the number of students with a student code of RE in academic year as a percentage of those with a student code of RE+ NE+ RP (repeat) + TI (transfer in) in the following academic year. This allows for those that join a cohort to be included in the progression rates of the stage.</p> $x = \frac{\text{No of Students at status 'R' with a student code of RE+RP+NE+TI in Academic Year-1}}{\text{No of students at status 'R' with student code of 'RE' in Academic Year}}$	
No. & percentage of students repeating on a programme		$x = \frac{\text{No of Students at status 'R' with a student code of 'RP'}}{\text{No of students at status 'R'}}$	Quercus

Indicator	Measure of/Proxy Measure	Definitions/Formula	Data Source
Overall progression/non-progression		<p><i>Limitations: This formula is currently problematic as students who commence a programme in January and are re-enrolled in September are tagged with an RP student code.</i> This can be mitigated if students are transferred rather than rolled</p> <p>Non progression of 1<sup>st</sup> year students is defined by the HEA as those students who do not return as a Re-enrolled (RE), transfer (TI), or Repeat (RP) student in stage 1 or 2 of any programme. This data is held in the studenthearecord, 'student code'</p> $x = \frac{\text{No of Students at status 'R' in Stage 1 with a student code of 'NE' in Academic Year-1}}{\text{No of students at status 'R' in Stage 1 and Stage 2 with student code of 'RE+RP TI in Academic Year'}}$	HEA SRS/Quercus
Pass/fail rates of a programme stage	<ul style="list-style-type: none"> <li>• Coherence of Programme Structure (sequential learning between stages)</li> <li>• Programme information for enrolled students (academic expectations of different stages)</li> <li>• Student attainment v. MIPLOs at stage level</li> </ul>	<p>Pass rates for a programme stage are defined as the number of students at status 'R' (registered) who have a passing grade at the end of all exam sittings as a percentage of those who were eligible to take assessment.</p> <p>2 sets of data are presented</p> <ol style="list-style-type: none"> <li>1. Rates which exclude those students who have an overall absent grade. (ABS)</li> <li>2. Rates which include all students.</li> </ol> <p>Those with an overall absent grade will have not submitted any assessment and are therefore assumed withdrawn, but have not officially done so and are therefore included. They may return in the following year.</p>	Quercus

Indicator	Measure of/Proxy Measure	Definitions/Formula	Data Source
Pass/fail rates of modules	<ul style="list-style-type: none"> <li>• Place of module in a programme</li> <li>• Student engagement for purposes of workload</li> <li>• Suitability of T&amp;L modes and assessment strategy</li> <li>• Problematic module combinations</li> </ul>	<p>Pass rates for a module are defined as the number of students at status 'R' (registered) and a subject registration status of 'REGISTERED' who have a passing grade at the end of all exam sittings as a percentage of those who were eligible to take assessment.</p> <p>2 sets of data are presented for each sitting of assessment</p> <ol style="list-style-type: none"> <li>1. Rates which exclude those students who have an overall absent grade. (ABS) or deferred grade (I)</li> <li>2. Rates which include all students.</li> </ol> <p>Those with an absent grade for a module will have not submitted any assessment and may be assumed withdrawn, but have not officially done so.</p>	Quercus
Max., Min., averages and standard deviations of module results	<ul style="list-style-type: none"> <li>• Marking spread per module, programme and school</li> <li>• Difficulty of module</li> </ul>	<p>The maximum, minimum and average mark per module of those that attempted the module.</p> <p>Used to look at specific cohorts and for module moderation</p>	Quercus
Final Award classifications of	<ul style="list-style-type: none"> <li>• Student attainment of MIPLOs</li> <li>• spread of grade classifications in Award Year</li> <li>• Trends between marking spreads of award year</li> </ul>	<p>Percentage of students who are awarded in the relevant award classification band</p>	Quercus

Indicator	Measure of/Proxy Measure	Definitions/Formula	Data Source
	<p>and previous years</p> <ul style="list-style-type: none"> <li>• trends of award classifications by programme and year</li> <li>• NCI award classifications v. national standards, HECA, and industry benchmarks</li> </ul>		
Bachelors Graduation Rate	<ul style="list-style-type: none"> <li>• Coherence of Programme</li> <li>• Sequential Learning between Stages</li> <li>• Suitability of T&amp;L modes and assessment strategy</li> <li>• Parity between MIPLOs and MIMLOs</li> <li>• Attainment rates of specific</li> </ul>	<p>The percentage of new entrants that successfully completed their bachelor programme. This links back to the issue of isolating a new entrant cohort.</p> $\frac{\sum \text{Graduates in level 8 programmes in academic year}}{\sum \text{new entrants in academic year } t - x}$ <p>Where t = year of graduation and x = programme duration Care should be taken to factor in part-time provision and longer duration times</p>	Quercus
Masters Graduation Rate		$\frac{\sum \text{Graduates in level 9 programmes in academic year}}{\sum \text{new entrants in academic year } t - x}$ <p>Where t = year of graduation and x = programme duration</p>	Quercus

Indicator	Measure of/Proxy Measure	Definitions/Formula	Data Source
Graduating on Time (Bachelor)	cohorts and/or demographics	Care should be taken to factor in part-time provision and longer duration times	
		The percentage of graduates that graduated within the time expected (normative time) for their bachelor programme  $\frac{\sum \text{Graduates of level 8 programmes within time expected}}{\sum \text{Level 8 degrees awarded}}$	Quercus
Graduating on Time (Master)		$\frac{\sum \text{Graduates of level 9 programmes within time expected}}{\sum \text{Level 9 degrees awarded}}$	Quercus
Graduate Outcomes	<ul style="list-style-type: none"> <li>• <b>Employability</b></li> <li>• <b>Programmes' suitability to industry requirements</b></li> <li>• <b>Student engagement with Employment and Opportunity Service</b></li> <li>• <b>Visibility and Integration of Employment and Opportunity Service</b></li> </ul>	Percentage of graduates who are working, in further study, travelling or seeking employment	Careers FD survey/CRM
ISSE indicators		As defined by the nationally co-ordinated survey of student engagement (ISSE)	ISSE

### 9.8.3 Student Engagement KPIs

Indicator	Measure of/Proxy Measure	Definitions/Formula	Data Source
Student attendance at learning events	<ul style="list-style-type: none"> <li>• Student engagement (academic)</li> </ul>		TDS
Student engagement with VLE	<ul style="list-style-type: none"> <li>• Relationship between student engagement and academic attainment</li> </ul>		Moodle
Student use of library resources	<ul style="list-style-type: none"> <li>• Suitability of T&amp;L modes and learning resources</li> </ul>		
Student presence in library			
Student use of support services Careers Learning Support Computer Support	<ul style="list-style-type: none"> <li>• Visibility of Student Support Services</li> <li>• Comms. Strategies of different services</li> </ul>		
No. student complaints	<ul style="list-style-type: none"> <li>• Student satisfaction</li> <li>• Quality of information provided to learners</li> </ul>		Registrar's Office – not systemised
No. disciplinary events	<ul style="list-style-type: none"> <li>•</li> </ul>		Registrar's Office – not systemised
No. disciplinary events upheld	<ul style="list-style-type: none"> <li>• Effectiveness of policies</li> <li>• Consistency of approach</li> </ul>		Registrar's Office – not systemised

#### 9.8.4 Internationalisation KPIs

Indicator	Measure of/Proxy Measure	Definitions/Formula	Data
			Source
No. international students	<ul style="list-style-type: none"> <li>• Effectiveness of International Recruitment Strategy</li> <li>• Trends within programmes and schools</li> </ul>	$X = \frac{\text{No students where student hea.study visa=true}}{\text{Full-time undergraduate + postgraduate students}}$ <p>The definition of an international student can be somewhat problematic. Using the proxy of the type of fee paid by a student does not automatically indicate that a student is indeed an international student.</p> <p>A student's domicile may not always indicate their status if they have been living in the country for a number of years. Therefore 'international' student for NCI purposes is defined as those students who are in Ireland on a study visa</p> <p>For HEA purposes and external reporting purposes , an international student is any student with a domicile not equal to Ireland</p> $X = \frac{\text{No students where student hea.hea domiciliary } \neq \text{ IE}}{\text{Full - time undergraduate + postgraduate students}}$	Quercus
No. Erasmus students	Internationalisation	$\frac{\text{No students where student hea.exchange} = (\text{EI or EO})}{\text{Full - time undergraduate + postgraduate students}}$	Quercus
No. students from international	Internationalisation	$\frac{\text{No students where application type} = \text{COLLABORATION}}{\text{Full - time undergraduate + postgraduate students}}$	Quercus

Indicator	Measure of/Proxy Measure	Definitions/Formula	Data Source
collaboration partners s	Relevance of articulation agreements		

#### 9.8.5 Widening Participation KPIs

Indicator	Measure of/Proxy Measure	Definitions/Formula	Data Source
Flexible Learners	Meeting mission  Contribution to sector  NCI independence of Govt funding for PT learners	$\frac{Part-time + distance + online + inservice}{All enrolments}$ $\frac{(PT + Distance + online inservice) - (Springboard + ICT + LMA)}{All enrolments}$	Quercus/HEA return
Participation in Labour Activation initiatives	Meeting mission  Dependence on Govt funding  National contribution to sector	$\frac{Springboard + ICT + LMA}{All enrolments}$ $\frac{Springboard + ICT + LMA}{Total Springboard + ICT + LMA nationally}$	Quercus HEA

Indicator	Measure of/Proxy Measure	Definitions/Formula	Data Source
Regional Intake	Meeting mission  Measure of contribution to local educational needs	For Irish domiciled students, Percentage of FT enrolments from Dublin or bordering counties  Number of full time students with a domicile of IE with a home address in Dublin, Kildare, Meath, Wicklow.  Number of full time students with a domicile of IE from DEIS schools  Number of full-time students with a domicile of IE from ETB/PLC colleges	Quercus
Mature Students	Meeting mission	Percentage of full-time new entrants who are 23 or over on the January preceeding entry	Quercus
Entrants with a disability	Meeting mission	Number of new entrants who indicate a disability	Quercus/SRS
Student supported by FSD	Meeting mission  Support of students	<i>No FT Postgraduate + Undergraduate student with FSD</i>  All FT enrolments	Quercus/SRS
Entrants from non manual, semi skilled or unskilled occupations	Meeting mission		

#### 9.8.6 Research and Knowledge Transfer KPIs

Indicator	Measure of/Proxy Measure	Definitions/Formula	Data Source
No doctoral graduates per 10 academic staff	Not currently relevant to NCI		

Indicator	Measure of/Proxy Measure	Definitions/Formula	Data Source
No Web of Science publications per academic			
No Scopus publications per academic			
Research Income			

#### 9.8.7 Staff KPIs

Indicator	Measure of/Proxy Measure	Definitions/Formula	Data Source
No. Core Staff Academic/Non Academic No Contract & Specialist Staff		Core staff are those employed on permanent contracts  Contract staff are those employed on fixed term contracts and includes associate faculty  1 FTE = 35 hours?	Core
Non academic/academic staff ratio		All non academic staff/all academic staff	Core
Academic Staff FT/PT ratio		All academic FT/all academic PT	Core
Age Profile of Staff			Core
Gender profile of staff	• Diversity • Engagement with Athena SWAN charter (2015)		Core
Gender profile of senior staff			Core
Staff Qualifications (highest qualification)	Meets ESG/QOI guidelines that those teaching are qualified to do so	Full-time academic staff with Masters  Full-time academic staff with Doctorate  All academic staff with Masters	Core

Indicator	Measure of/Proxy Measure	Definitions/Formula	Data Source
		All academic staff with Doctorate	
Student to academic staff ratio			Core/Quercus

#### 9.8.8 Financial KPIs

Indicator	Measure of/Proxy Measure	Definitions/Formula	Data Source
Total income			Sun
Total expenditure			Sun
Pay cost			Sun
Non pay cost			Sun
Expenditure per student		Adjusted Total Expenditure (adjusted for pensions funding & depreciation) per student numbers as used in SRS	



## 9.9. APPENDIX 9-2: DATA RETENTION SCHEDULES

Student Records					
Function/Unit	Record Type	Trigger	Retention Period	Action	Comments/Notes
Application	Unsuccessful applications	End of appeal period	1 year	Destroy	Sample records include application forms, interview records, correspondence, etc.
	Successful applicants who do not register	Intended registration date	1 year	Destroy	
	Registration records	Completion of studies	1 year	Destroy	Relates to routine records such as correspondence, fees, etc.
Student Record	Variation to studies	Completion of studies	1 year	Destroy	Includes deferral, discontinuation, transfer, etc.
	Variation to personal details	Completion of studies	1 year	Destroy	Includes change of address, contact details, etc.
	Attendance	Completion of studies	1 year	Destroy	
	Credit bearing placements	Completion of studies	1 year	Destroy	Record of placement remains on the student record, operational matters and correspondence etc is removed
Discipline	Disciplinary Records - major incidents	Completion of studies	Permanent	Archive	
	Disciplinary Records - minor incidents	Completion of studies	6 years	Destroy	
Support & Welfare	Medical/Health	According to specific nature of record	As required	Destroy	Retention for minimum period necessary to particular case or circumstances
	Disability support services	Completion of studies	1 year	Destroy	
	Other student support services	According to specific nature of record	As required	Destroy	Retention for minimum period necessary to particular case or circumstances
Assessment	Examination papers and Continuous Assessment Briefs	End of programme	5 years	Destroy	Includes Moodle quiz and other assessment types
	Examination scripts and Continuous Assessment Submissions	End of appeal period	13 months	Destroy	Includes Moodle quiz and other assessment types
	Requests for extensions and extenuating circumstances	End of appeal period	13 months	Destroy	
	External examiners' reports	End of programme	5 years	Destroy	
	Transcripts/Final Results	Completion of studies	Permanent	Archive	
Awards	Postgraduate theses	Date of submission	Permanent	Archive	Retain in Library
	Student awards and prizes	Date of award	Permanent	Archive	
	Graduation/conferring records	Date of event	Permanent	Archive	
	Register of Graduates	n/a	Permanent	Archive	
Governance Records					
Function/Unit	Record Type	Trigger	Retention Period	Action	Comments/Notes
Executive Board	Minutes	End of academic year	5 years	Archive	Single official record to be held by designated office holder, with access available to all authorised officers. Duplicates to be
	Agenda	End of academic year	5 years	Archive	
	Supporting Documentation	End of academic year	5 years	Archive	
Governing Body	Minutes	End of academic year	5 years	Archive	Single official record to be held by designated office holder, with access available to all authorised officers. Duplicates to be
	Agenda	End of academic year	5 years	Archive	
	Supporting Documentation	End of academic year	5 years	Archive	



## **National College of Ireland Privacy Statement**

NCI-Privacy- Statement

Last Updated May 2018

## Version Control

<b>Document Name:</b> Privacy Statement	
<b>Owner:</b> Acting Data Protection Officer	
<b>Approved by:</b>	
<b>Review frequency:</b> Annually	 <b>National College of Ireland</b>

<b>Version Number</b>	<b>Version Date</b>	<b>Revised by</b>	<b>Description</b>
001	17/05/2018	Arthur Cox	For NCI Final Review & Internal Approval
002	22/05/2018	NCI	Internal Review
003	24/05/2018	NCI	Incorporating both internal & AC feedback

## **1. Introduction & Scope**

1.1 The National College of Ireland is referred to in this Privacy Statement as “**NCI**”, “**us**” or “**we**”. This Privacy Statement provides details of how and why we Process Personal Data in line with our obligations under Data Protection Law. This statement applies to all individuals whose Personal Data is Processed by NCI except for NCI staff who should refer to NCI’s Staff Data Processing Notice, which is available on request from NCI’s acting data protection officer (see section 15 below for contact details).

## **2. Background and Purpose**

- 2.1 The purpose of this Privacy Statement is to explain what Personal Data we Process and how and why we Process it. In addition, this Privacy Statement outlines our duties and responsibilities regarding the protection of such Personal Data.
- 2.2 This Privacy Statement is not an exhaustive statement of our data protection practices or policies. The manner in which we Process Personal Data will evolve over time and we will update this Policy from time to time to reflect changing practices and changes to the law. In addition, we operate a number of other workplace policies and procedures which inter-relate with this Privacy Statement, including the following:
- (a) Data Protection Policy;
  - (b) Data Retention Policy;
  - (c) Website Privacy Statement; and
  - (d) Staff Data Processing Notice.
- 2.3 In addition, in order to meet our transparency obligations under Data Protection Law, we will incorporate this Privacy Statement by reference into notices used at various points of data capture when collecting Personal Data (e.g. application forms, website forms etc.).

## **3. NCI as a Data Controller**

- 3.1 When NCI determines the purposes and means of the Processing of Personal Data it acts as a Data Controller. The primary example is where NCI collects and processes Personal Data relating to NCI students. In relation to such processing, NCI relies on a number of legal bases under Data Protection Law. These include:
- (a) Art. 6(1)(a) of the GDPR which permits Processing where the data subject has given his or her consent;
  - (b) Art 6(1)(b) which permits Processing where necessary for the performance of a contract to which the data subject is a party;
  - (c) Art. 6(1)(c) which permits Processing that is necessary for compliance with a legal obligation to which the Data Controller is subject;
  - (d) Art. 6(1)(d) which permits Processing that is necessary in order to protect the vital interests of the data subject or of another person; and
  - (e) Art. 6(1)(f) which permits Processing pursuant to the legitimate interests of NCI or a third party.
- 3.2 In certain instances NCI will act as a joint controller of Personal Data (“**Joint Controller**”), whereby NCI together with other entities determines the means and purposes of the relevant Processing. In such circumstances the essence of the arrangement is between NCI and the other Joint Controllers will be made known to the relevant individuals in a transparent manner. Examples of such scenarios may include where NCI and other institutions engage in collaborative research projects.

#### **4. NCI as a Data Processor**

4.1 In some cases, NCI may act as a Data Processor, under the instructions of a Data Controller. When acting as a Data Processor, NCI complies with its relevant obligations under Data Protection Law. These include ensuring that the data that is Processed by NCI on behalf of the relevant Data Controllers is subject to appropriate technical and organisational measures to ensure a level of security appropriate to the risk and ensuring that the Processing is underpinned by a contract which includes the data protection provisions required by Data Protection Law.

#### **5. Purposes of Processing**

5.1 Much of the data Processing undertaken by NCI is for the purpose(s) of fulfilling NCI's contractual obligations in respect of its students to provide both undergraduate, postgraduate and professional courses and qualifications across a range of disciplines. The following are illustrative and non-exhaustive examples of the types of Processing typically undertaken by NCI when providing courses of education and for connected purposes:

- (a) **Student Registration:** In administering the college it is necessary for NCI to Process Personal Data, including contact details and financial details of students. This is necessary in relation to NCI's contractual relationship with its students.
- (b) **Examinations and Academic Records:** The Processing of Personal Data, including but not limited to student numbers, names, exam scripts, exam results, details of qualifications and degrees conferred is necessary in order for NCI to perform its contractual obligations. To ensure the integrity of this system, it is also necessary and proportionate for NCI to maintain records of exam results, degrees conferred and other relevant details. NCI Processes such Personal Data in accordance with this Privacy Statement and its other policies and procedures.
- (c) **Research and Publications:** NCI Processes Personal Data in the course of its research and publishing activities and such Processing is always undertaken in accordance with this Privacy Statement and NCI's legitimate interests in publishing and disseminating certain information and research.
- (d) **Alumni Affairs:** Processing activities undertaken by NCI's Alumni Office when liaising with and contacting NCI graduates in relation to their alumni events and initiatives are necessary for the performance of NCI's legitimate interests to maintain contact with alumni and to promote NCI.
- (e) **NCI Students Union:** The NCI Students Union is the representative body for NCI students and NCI actively collaborates with the Students Union on various initiatives. This is necessary for NCI's legitimate interests in fostering an inclusive and vibrant student body.
- (f) **SV Fitness:** SV. Fitness Health Club: S.V. Fitness Health Club ("S.V. Fitness") makes health and fitness services available to all NCI students. It is a term of NCI full-time undergraduate registration that students are enrolled as members of S.V. Fitness. In order for S.V. Fitness to make such services available to NCI students, NCI shares with S.V. Fitness certain NCI student personal data, including student names and student numbers. Of course, you may also provide other data to S.V. Fitness in connection with your gym membership. S.V. Fitness will act as data controller in respect of all data that it holds and processes relating to NCI students and will process such data only for purposes connected with your membership.

- (g) **Other institutions:** NCI will engage in certain collaboration with educational, business and other institutions both within and outside the State. Such collaborations may involve the sharing of certain Personal Data as between NCI and its partner institutions and other organisations for research purposes and for similar purposes including staff sabbaticals. Personal Data of students and staff may be disclosed to such other institutions as necessary for these purposes and written agreements will be put in place.
- (h) **Student Support:** NCI students and employees provide information to NCI for a variety of reasons when availing of the student support services. Such information may include Personal data of a sensitive nature (known as “special categories of Personal Data”) including details of disabilities, health, sex life and/or sexual orientation and of your background. Such Personal Data may be collected in the form of records of meetings and disability records, counselling notes, records of financial assistance provided, health and disability records as well as workshop and event attendance records. Such data will be collected based on your explicit consent and otherwise to protect the vital interests of the data subject and/or third parties and where it is necessary in order for NCI to comply with any legal obligations it may have. Given the potentially sensitive nature of the Personal Data collected and processed by NCI special care is taken to maintain the security and confidentiality of such data. Such data will not be disclosed to third parties outside of NCI except in exceptional circumstances such as an emergency or a valid request from law enforcement.
- (i) **NCI Early Learning Initiative (“ELI”):** NCI’s ELI operates a number of programmes which involves active participation and engagement within the local community. These programmes involve NCI staff working with parents/guardians and young children in family homes and/or within NCI and the local community. The ELI programmes involve the processing of Personal Data to administer the programme and to monitor the progress and participation levels of those participating in the ELI programmes. The legal bases for this is consent of the participating families (as provided by the parents / guardians on behalf of their children) and or the legitimate interests pursued by NCI in undertaking and promoting educational initiatives within the local community.

## **6. Special Categories of Data**

- 6.1 NCI processes Special Categories of Data (“SCD”) in certain circumstances, typically related to the ordinary course of employee and student administration, the provision of student support, early learning initiatives and development services and the processing of Garda vetting forms for students and employees, where required by law.
- 6.2 Section 45 of the Data Protection Act 2018 provides a general lawful basis for processing SCD where it is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the controller or the data subject in connection with employment or social welfare law. As required by Data Protection Law, NCI applies suitable and specific measures in respect of such Processing of SCD.
- 6.3 NCI Processes Garda vetting forms for employees as authorised by the National Vetting Bureau (Children and Vulnerable Persons) Act 2012 to 2016 (the “**National Vetting Act**”) in respect of staff and students that undertake placements and studies which involves engagement with and exposure to children and/or vulnerable persons. Garda vetting forms may contain Personal Data relating to criminal convictions/offences and because NCI is subject to a legal obligation to Process such data and Art. 6(1)(c) of the GDPR provides the lawful basis for such Processing.

## 7. Record Keeping

7.1 As part of our record keeping obligations under Art. 30 of the GDPR, NCI retains a record of the processing activities under its responsibility. This comprises the following:

Art. 30 GDPR Requirement	NCI Record
• Name and contact details of the controller	• National College of Ireland, IFSC, Mayor Street, North Dock, Dublin 1, D01 Y300.
• Name and contact details of the acting data protection officer	• Geraldine Minogue, • Email: <a href="mailto:dpo@ncirl.ie">dpo@ncirl.ie</a> • Telephone: +353 1 4498541
• The purposes of the processing.	• To fulfil the functions of NCI as described in this Privacy Statement (see Section 5 and Annex II).
• Description of categories of data subjects and Personal Data.	• See Annex II.
• The categories of recipients to whom the Personal Data have been or will be disclosed.	• See Section 12.
• Transfers of Personal Data to a third country outside of the EEA.	• On occasion Personal Data may be transferred to other institutions for the purposes of collaborative research projects.
• Envisaged time limits for erasure of the different categories of data.	• See Section 13.
• General description of the technical and organisational security measures referred to in Article 32(1).	• See Section 11.

## 8. Individual Data Subject Rights

8.1 Data Protection Laws provide certain rights in favour of data subjects. The rights in question are as follows (“**Data Subject Rights**”):

- (a) The right of a data subject to receive detailed information on the processing (by virtue of the transparency obligations on the Controller);
- (b) The right of access to Personal Data;
- (c) The right to rectify or erase Personal Data (right to be forgotten);
- (d) The right to restrict Processing;
- (e) The right of data portability;
- (f) The right of objection; and
- (g) The *right to object to* automated decision making, including profiling and where processing is based on the Controller’s legitimate interests.

8.2 Please note that the Data Subject Rights will not be available in all circumstances and are subject to certain conditions.

- 8.3 Any data subject wishing to exercise their Data Subject Rights should write to NCI'S Acting Data Protection Officer ("DPO") by post to the National College of Ireland, IFSC, Mayor Street, North Dock, Dublin 1, D01 Y300, or by email at [dpo@ncirl.ie](mailto:dpo@ncirl.ie). Please provide as much detail as possible in relation to your request to enable us to identify your personal data and facilitate your request.

## **9. Academic Freedom and Freedom of Expression Information**

- 9.1 While NCI will take all appropriate and reasonable measures to respect and facilitate the protection rights of the individual whose Personal Data it processes, data protection is not an absolute right and must be balanced against certain other rights and principles. The GDPR and the Data Protection Act 2018 recognise that in certain circumstances it may be necessary to limit data protection rights in the interests of freedom of expression and the freedom to receive information. In performing its tasks as an educational institution, it is the policy of NCI to endeavour to protect these freedoms in a manner that least impacts on the data protection rights of individuals.

## **10. CCTV on the NCI Campus**

- 10.1 NCI has closed circuit television cameras ("CCTV") located throughout its premises covering buildings, internal spaces, car parks, roads, pathways and grounds. NCI's CCTV system is implemented in a proportionate manner as necessary to protect NCI property against theft or pilferage and for the security of staff, students and visitors to the NCI premises to protect their vital interests.
- 10.2 Whilst CCTV footage is monitored by NCI security staff, and other authorised personnel access to recorded footage is strictly limited to authorised personnel. Footage is retained for 30 days, except where incidents or accidents have been identified in which case such footage is retained specifically in the context of an investigation of that issue. CCTV footage may be used in the context of disciplinary proceedings involving NCI staff or students (to protect the vital interests of NCI, staff, students and affected individuals). CCTV footage is not disclosed to third parties except where disclosure is required by law (such as for the purpose of preventing, detecting or investigating alleged offences) and in such instances disclosure is based on a valid request. Signage indicating that CCTV is in use is displayed prominently throughout the NCI premises. For information on CCTV operations at NCI please contact Mr Bertie Kelly by email at [bkelly@ncirl.ie](mailto:bkelly@ncirl.ie).

## **11. Data Security and Data Breach**

- 11.1 We have technical and organisational measures in place to protect Personal Data from unlawful or unauthorised destruction, loss, change, disclosure, acquisition or access. Personal Data are held securely using a range of security measures including, as appropriate, physical measures such as locked filing cabinets, IT measures such as encryption, and restricted access through approvals and passwords.
- 11.2 The GDPR obliges Data Controllers to notify the Data Protection Commission and affected data subjects in the case of certain types of Personal Data security breaches. We will manage a Data Breach in accordance with the Data Breach Incident Procedure. To report a suspected Data Breach please immediately contact the NCI DPO at the contact details at Section 7.1 above.

## **12. Disclosing Personal Data**

- 12.1 From time to time, we may disclose Personal Data to third parties, or allow third parties to access Personal Data which we Process (for example where a law enforcement agency submits a valid request for access to Personal Data). We may also share Personal Data: (a) with statutory bodies, such as the Higher Education Authority where there is a lawful basis to do so; (b) with selected third parties including sub-contractors; (c) if we are under a legal obligation to disclose Personal Data (e.g. to the Gardaí).
- 12.2 Where we enter into agreements with third parties to Process Personal Data on our behalf we will ensure that the appropriate contractual protections are in place to safeguard such Personal Data. Examples of such third party service providers that we engage, and to whom Personal Data may be disclosed, include but are not limited to communications providers, payroll service providers, occupational health providers, marketing or recruitment agencies, operators of data centres used by us, security providers, catering services, and professional advisors such as external lawyers, accountants, tax and pensions advisors.

## **13. Data Retention**

- 13.1 We will keep Personal Data only for as long as the retention of such Personal Data is deemed necessary for the purposes for which that Personal Data Are Processed. Further details of the retention period for Personal Data is set out in our Data Retention Policy.

## **14. Data Transfers outside the EEA**

- 14.1 From time to time we may transfer Personal Data outside the EEA. Such transfer will be subject to appropriate safeguards in accordance with applicable Data Protection Law (for example through the use of EU-approved Model Contract Clauses) and in accordance with this Privacy Statement. An example of where we transfer Personal Data outside the EEA is for the purpose of collaborative research projects with other institutions.

## **15. Further Information/Complaints Procedure**

- 15.1 For further information about this Privacy Statement and/or the Processing of your Personal Data please contact NCI's Acting Data Protection Officer, Geraldine Minogue, at [dpo@ncirl.ie](mailto:dpo@ncirl.ie). While you may make a complaint in respect of our compliance with Data Protection Law to the Irish Data Protection Commission, we request that you contact the Data Protection Officer in the first instance to give us the opportunity to address any concerns that you may have.

## ANNEX I - GLOSSARY

In this Privacy Statement, the terms below have the following meaning:

**“Data Breach”** means 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.

**“Data Controller”** means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

**“Data Processor”** means the party that Processes Personal Data on behalf of the Data Controller (for example, a payroll service provider).

**“Data Protection Law”** means the General Data Protection Regulation (No 2016/679) (“**GDPR**”) and the [Data Protection Act 2018] and any other laws which apply to NCI in relation to the Processing of Personal Data.

**“European Economic Area”** or **“EEA”** means Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, the UK, Iceland, Liechtenstein, and Norway.

**“Personal Data”** is any information relating to a living individual which allows the identification of that individual. Personal Data can include a name, an identification number; details about an individual’s location; or any other information that is specific to that individual.

**“Processing”** means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. **“Process”** and **“Processing”** are interpreted accordingly.

**“Special Categories of Personal Data”** are types of Personal Data that reveal any of the following information relating to an individual: racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. Special Categories of Personal Data also include the Processing of genetic data, biometric data (for example, fingerprints or facial images), health data, data concerning sex life or sexual orientation and any Personal Data relating to criminal convictions or offences.

## ANNEX II - TYPES OF PERSONAL DATA

*The following table indicates the categories of Personal Data typically Processed by NCI but we may Process other categories of Personal Data from time to time and will endeavour to provide you with a privacy notice whenever we collect other Personal Data.*

Type of Personal Data	Purpose	GDPR Lawful Basis for Processing
<b>A. STUDENT REGISTRY DATA</b>		
<ul style="list-style-type: none"> <li>• Name, contact details, student ID number;</li> <li>• date of birth, gender, next of kin, nationality, photograph, admission and application record, student grant information;</li> <li>• PPSN, passport number, student grant information (which may include SCPD), bank details, nationality;</li> <li>• Academic records, examination materials, graduation record;</li> <li>• Health and medical data;</li> <li>• Data relating to criminal offences contained in Garda vetting forms; and</li> <li>• Facial images on student and staff access cards.</li> </ul>	Data is processed for: <ul style="list-style-type: none"> <li>• student registration, provision of financial support and administration, examinations and ancillary services such as student support and development;</li> <li>• administering payment of fees, student registration, provision of student grants and funding, administration of exams and student communications;</li> <li>• department administration (such as module registration and payment of fees); and</li> <li>• for security purposes and as necessary for the conduct of examinations and student attendance purposes.</li> </ul>	Necessary for performance of a contract under Art. 6(1)(b) GDPR; and  Performance of NCI's legitimate interests under Art. 6(1)(f) GDPR.
<b>B. OTHER STUDENT DATA</b>		
<ul style="list-style-type: none"> <li>• NCI Sport clubs and societies;</li> <li>• Health and medical data;</li> <li>• Health data, such as details of health conditions or disabilities in case of emergencies; and</li> <li>• Student next of kin contact details.</li> </ul>	<ul style="list-style-type: none"> <li>• Access to amenities such as sports facilities and contacting next-of-kin in emergencies/accidents;</li> <li>• ancillary services for students such as clubs and societies; and</li> <li>• Student registration and exam purposes (e.g. extenuating circumstances).</li> </ul>	Consent under Article 6(1)(a); and  Necessary to protect the vital interests of the data subject under Art. 6(1)(d).
<b>C. VISITORS TO NCI CAMPUS &amp; EVENTS</b>		
<ul style="list-style-type: none"> <li>• Names and details of conference, meeting and work-shop attendees and photographs taken at events;</li> <li>• Parents of students; and</li> <li>• Other visitors.</li> </ul>	<ul style="list-style-type: none"> <li>• Administration of conferences and for promotional purposes in relation to photographs taken;</li> <li>• Open days; and</li> <li>• CCTV surveillance of NCI premises.</li> </ul>	Consent under Article 6(1)(a); and  Performance of NCI's legitimate interests under Art. 6(1)(f) GDPR.

**D. EMPLOYEES\***

\*Refer to the Staff Data Processing Notice

**E. SUPPLIERS, CONTRACTORS AND BUSINESS CONTACTS**

<ul style="list-style-type: none"> <li>• Name, contact details of suppliers, contractors and business contacts</li> <li>• Personal Data relevant to performance of contract</li> </ul>	<ul style="list-style-type: none"> <li>• Performance of services / supply of goods; and</li> <li>• Maintenance of customer relationship management (or CRM) system.</li> </ul>	Consent under Article 6(1)(a); Necessary for performance of a contract under Art. 6(1)(b) GDPR; and Necessary for the legitimate interests pursued by NCI under Art. 6(1)(f).
--	--	---

**E. RESEARCH & ACADEMIC PURPOSES**

<ul style="list-style-type: none"> <li>• Staff details, external and visiting academics and teaching staff;</li> <li>• Contacts with other educational institutions, journals; and</li> <li>• Research participants in trials / studies.</li> </ul>	Administration and coordination of research and publication. Conferences and related academic purposes.	Necessary for performance of a contract under Art. 6(1)(b) GDPR; Necessary for the legitimate interests pursued by NCI under Art. 6(1)(f); and Consent under Article 6(1)(a).
---	---	---

**F. WEBSITE VISITORS\***

<ul style="list-style-type: none"> <li>• IP address, online identifiers, device, and browser; and</li> <li>• Location of device.</li> </ul>	Technology such as cookies help us understand which parts of our website are the most popular and how much time visitors spend on the site.  NCI also uses cookies to study traffic patterns on our site in order to improve website performance, to customise the user experience, and to better match the users' interests and preferences.	Necessary for the legitimate interests pursued by NCI under Art. 6(1)(f).
---	---	---

*\*For further information please refer to our Cookies Policy.*