



ICHAS

Section 9 - Information & Data Management

Subject:	Policy on Data Collection, Usage & Management		
Applicable Standard	QQI	Core	Information And Data Management
Date Approved by Academic Council:			August 2021
Policy Version	1/2019	Date due for Revision	February 2024

CONTEXT

ICHAS has an obligation to abide by all Irish legislation and relevant legislation of the European Community, together with a number of public sector specific guidelines or standards. Relevant legislation includes but is not limited to:

- General Data Protection Regulation (2018)
- The Data Protection Act (1988/2003)
- European Communities Data Protection Regulations, (2001)
- European Communities (Data Protection and Privacy in Telecommunications) Regulations (2002)
- Data Protection EU Directive 95/46/EC
- Criminal Damages Act (1991)
- Child Trafficking and Pornography Act (1998)
- Intellectual Property Miscellaneous Provisions Act (1998)
- Copyright and Related Rights Act (2000)
- Criminal Justice (Theft & Fraud Offences) Act 2001
- Electronic Commerce Act (2000)
- E-Commerce Directive (2000/31/EC)
- The EU General Data Protection Regulation (2016/679)
- Freedom of Information Acts 1997,2003 & 2014

POLICY STATEMENT

The College only collects and processes data that it is lawfully permitted to collect; that is relevant to the functions of the College and that is necessary for statutory, regulatory purposes and/or necessary for obligations that the College may have for professional accreditation purposes or similar requirements. ICHAS recognises its responsibility under the Freedom of Information Acts 1997,2003 & 2014 and the right of students or

anyone whose data is stored and maintained by ICHAS to gain access to information held on them by the College and will comply with any legitimate requests made under the Acts.

ICHAS is committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller and the handling of such data in line with the data protection principles and the Data Protection Act (DPA).

Changes to data protection legislation shall be monitored and implemented in order to remain compliant with all requirements.

All member(s) of staff are responsible for data protection with specific management of compliance by suitably qualified individuals (IS Manager, Information Technology Manager, QAE Officer etc.). The College is also committed to ensuring that its staff are aware of data protection policies, legal requirements and adequate training is provided to them. The requirements of this policy are mandatory for all staff employed by the College and any third party contracted to provide services at the College.

Notification

If necessary, the College will register the data processing activities with the Data Commissioner's Office as required of a recognised Data Controller. Changes to the type of data processing activities being undertaken shall be notified to the Data Protection Commissioners and details amended in the register.

Breaches of personal or sensitive data shall be notified immediately to the individual(s) concerned and the Data Protection Commission.

Personal and Sensitive Data

All data within the ICHAS College's control shall be identified as personal, sensitive or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

The definitions of personal and sensitive data shall be as those published by the Data Protection Commission for guidance – key definitions are outlined in the accompanying procedure. The principles of the Data Protection Act shall be applied to all data processed:

1. Processed fairly and lawfully.
2. Obtained only for lawful purposes, and is not further used in any manner incompatible with those original purposes.
3. Accurate and, where necessary, kept up to date,
4. Adequate, relevant and not excessive in relation to the purposes for which it is processed.
5. Not kept for longer than is necessary for those purposes.
6. Processed in accordance with the rights of data subjects under the Data Protection Acts
7. Protected by appropriate technical and organisational measures against

unauthorised or unlawful processing and against accidental loss, destruction or damage.

8. Not transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection of the personal information

Fair Processing / Privacy Notice:

The College shall be transparent about the intended processing of data and communicate these intentions via notification to staff and students prior to the processing of individual's data. Notifications shall be in accordance with the Data Commissioners guidance and, where relevant, be written in a form understandable by those defined as 'Children' under the legislation.

The intention to share data relating to individuals to an organisation outside of the College shall be clearly defined within notifications and details of the basis for sharing given. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information. Any proposed change to the processing of individual's data shall first be notified to them.

Data Security

In order to assure the protection of all data being processed and inform decisions on processing activities, we shall undertake an assessment of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them.

Risk and impact assessments shall be conducted in accordance with guidance given by the Data Protection. Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance.

The security arrangements of any organisation with which data is shared shall also be considered and these organisations shall provide evidence of the competence in the security of shared data.

Data Access Requests (Subject Access Requests):

All individuals whose data is held by the College, has a legal right to request access to such data or information about what is held.

Data Disposal

The College recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process. Disposal of IT assets holding data shall also be in compliance with data protection guidance.

SCOPE

Applies To	Staff	Students	Both	
			✓	
Responsible for Implementation	Information Systems Manager			
Responsible for Monitoring & Review	Vice President (Corporate Affairs)	Vice President (Academic Affairs)	Registrar	Quality Assurance & Enhancement Officer
	✓	✓		✓

RELEVANT GUIDELINES/ POLICIES INFORMING THIS POLICY

- Government of Ireland (2018) Data Protection Act
- European Association for Quality Assurance in Higher Education (ENQA) et al (2015) Standards and Guidelines for Quality Assurance in the European Higher Education Area (ESG).
- Quality and Qualifications Ireland (2016) Sector Specific Statutory Quality Assurance Guidelines Developed by QQI For Independent/Private Providers Coming To QQI On A Voluntary Basis
- Government of Ireland (2012) Qualifications & Quality Assurance (Education and Training Act).

Linked Policies and Procedures

Linked Policies	Policy on Public Information Policy on Access, Applications and Admissions Policy on Recognition of Prior Learning
Linked Procedures	Procedures associated with Public Information Procedures associated with Data Collection, Usage & Management Procedure Associated with Access and Admissions Procedure Associated with Recognition of Prior Learning