ICHAS

Section 9 - Information & Data Management

Subject:	Procedures associated with Data Collection, Usage & Management		
Date Approved by Academic Council:			**August 2021**
Policy Version	1/2021	Date due for Revision	February 2024
Parent Policy	Policy on Data Collection, Usage & Management		

INTRODUCTION

The College acquires, processes, and stores personal data in relation to

- Current and former employees
- Current and former students/ graduates
- Applicants
- Third parties engaged with the College.

ICHAS is committed to the protection of all personal and sensitive data which it holds, and this is the responsibility of the Data Controller (s) at the College. The handling of such data is in line with the data protection principles and the General Data Protection Regulations (GDPR). All member(s) of staff are responsible for data protection with specific management of the compliance by the Data Protection Officer at the College. This function is undertaken by the Vice President (Corporate Affairs). 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.

Data is stored and managed securely in compliance with legislative and ´good practice´ requirements and guidelines. Data collected is used to inform decision making, for the purposes of making summary reports, or for enacting organisational and technical measures to ensure best practice.

RESPONSIBILITIES

ROLE/ PERSON	
Data Protection Officer	Management of the compliance with all GDPR policies. Communicate and put in place the necessary GDPR procedures for the management, collection, and usage of all data of the college
Data Controller (s) at the College	All staff are considered data controllers under this policy. They are required to ensure that all data is managed in line with GDPR requirements.
Students	Must be familiar with the requirements of GDPR from a student perspective.
Information Systems Manager	Work with the Data Protection Officer to implement the policy.
QAE Officer	Responsibility for the QA of the controls implemented and reporting of their performance.

Definitions
All definitions are derived from the Data Protections Acts.

Personal Data
The definition in the Data Protection Acts reads: "*personal data" means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller*;

A similar definition is contained in the EU Data Protection Directive (95/46/EC): "*personal data" shall mean any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*.

Manual Data and what is a Relevant Filing System
The definitions in the Acts read: *"manual data" means information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system*;" and, "*relevant filing system" means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible*;"

Back-up systems
Back-up data are defined in the Data Protection Acts, 1988 & 2003 as being.

"data kept only for the purpose of replacing other data in the event of their being lost, destroyed or damaged".

In order to fall within the definition of 'back-up data', data cannot be part of a live system, nor can they be used for any purpose other than replacing lost, destroyed or damaged data.

PROCEDURES

Collection & Processing of Data

Data Collection

- All Information Systems users at ICHAS are required to read and accept the conditions of use of information and data prior to being granted access to ICHAS information systems.
- All data within the College's control is identified as either personal, sensitive or both and will be 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 & sensitive data is as those published by the Data Protection Commission.
- College Staff receive training and routine updates relating to the requirements regarding Information and data that it collects, uses, and manages.
- The College is transparent about the intended processing of data and communicate these intentions via notification to staff and students (including applicants) prior to the processing of individual's data.
- Images (including classroom recordings) of staff and students can be captured at appropriate times and as part of educational activities for use in the College only with their consent.
- Unless prior and informed consent from staff and students has been given, the College will not utilise such images for publication or communication to external sources.
- Any unauthorised sharing of images or recorded material will be treated as a breach of GDPR and viewed as a breach of conduct.
- It is the College's policy that external parties cannot capture images of staff or students during such activities without prior consent.

Data Access

- All individuals whose data is held by the College, have a legal right to request access to such data or information about what is held therefore the College will respond to such requests within 40 days.
    - All requests of this nature should be made in writing to the Vice President (Corporate Affairs). A charge may be applied for processing the request.
    - The College will log the date of receipt of the valid request.
    - The Programme Co-ordinator will monitor the process of responding to the request – observing time limit of 40 days.
    - In order for a request to access can be processed a check has to be done to ensure that sufficient material has been supplied to definitively identify the individual See Policy and procedure section on Student Identity Verification in Policy and

Procedures for Ensuring the Quality of Online Only Learning Environment

- Sufficient information to locate the data must be supplied on request and if it is not clear what kind of data is being requested then the data subject has to be contacted for more information.
- The College will keep note of all steps taken to locate and collate data – if different divisions of the College are involved, have the steps "signed off" by the appropriate person.
- The Co-ordinator will supply the data in an intelligible form (include an explanation of terms if necessary). A description of purposes, disclosures, and source of data (unless revealing the source would be contrary to the public interest) will be provided and the documents provided will be number if necessary. This final document will be "signed-off" by an appropriate person.

In accordance with Section 5 of the Data Protection Acts the following exemptions to the right to access apply:

- Where the data being held is being used by bodies such as the Gardaí for the prevention, detection, investigation, or prosecution of a crime, or to prevent fraud.
- If the data is subject to legal professional privilege, meaning the data was created following legal advice from a solicitor, and/or the data was created specifically for an upcoming court case.
- Where the requester is involved in a claim against an organisation, seeking compensation, and the information reveals details of the organisation's decision process in relation to their claim.
- If the information is held for statistical purposes, is not shared with any other person or organisation, and cannot be identified as belonging to any particular individual.
- If releasing the data would mean that personal data about another individual would be unfairly disclosed. (Personal data may be released in redacted form to protect the other individual's data.)
- Where the data being sought involves personal opinions that have been expressed by another individual. Specifically, if the opinion was given in confidence, and it can be proven that the person providing the opinion at the time did so in the expectation of confidence, it does not have to be released. (If the opinion was given as part of regular business communications, does not involve personal opinions, and was given without the expectation of confidentiality, it should be released.)
- In the case of a request for access to personal medical information or social work records, access may be denied if there is reason to believe that releasing the information may cause serious risk to the physical or mental health of the individual. The decision not to release such data must be made after consulting the medical professional(s) most recently responsible for the care/ treatment of the data subject.
- If the personal data requested is impossible to supply or supplying, it would be extremely difficult (disproportionate effort).
- If the personal data has already been supplied in accordance with an access request, but identical requests continue to be made (unless new data has been created since the previous records were released, in which case the updated data must be provided).
- If the data that is requested is not the personal data of the requester, it cannot be released under an access request.

Changes and Restrictions to Data

- Any proposed change to the processing of individual's data will first be notified to them.
- Notifications are in accordance with the Data Commissioners guidance and, where relevant, be written in an understandable form
- Any intention to share data relating to individuals to an organisation outside of the College is clearly defined within notifications and details of the basis for sharing given.
- If the individual believes that their personal data is being used for a purpose of which they were not aware of and did not consent to, they can ask to have the use of their personal data restricted to the main purpose for which they originally supplied it.
- The right to change data will normally be restricted to the following:
    - factually incorrect (or no longer factually correct)
    - was obtained or processed in an unfair way.
    - is not kept accurate, complete and up-to-date.
    - is being used in a way that is not in keeping with the reason for which it was originally collected.
    - the data is being stored in an unsafe way, or the storage security measures are inappropriate.
    - the organisation cannot provide a valid reason to keep it.
    - the individual can ask to have the data corrected or deleted.

Sharing Data

- Data will be shared with external parties in compliance with the Policy parameters.
- Documents requested and summoned by legally authorized personnel will be provided within five working days.
- The Board of Management will authorize provision in such instances.
- No documents will be concealed, altered or destroyed with the intent to obstruct the investigation or litigation.
- ICHAS in its role as Data Controller, ensures that an agreement has been drawn up in advance of data being shared and that there are joint controllers of data involved.
- Currently joint controllers of data with ICHAS include Quality and Qualifications Ireland (QQI), Central Applications Office (CAO), Revenue Commissioners, Department of Social Protection and Department of Justice (INIS services) and the HECA PEL Scheme.
- Each controller is made aware of their obligations in relation to personal data, the specific purpose or purposes for which it is collected, processed, retained and transmitted and the need to implement GDPR rules when processing this type of data.
- Risk and impact assessments of data processing activities are conducted in accordance with guidance given by the Data Protection regulations.
- Regular review of the procedures and processes involved will be carried out.

Storage of Data and Data Security

All of ICHAS's information systems are subject to the Information Technology Security standards as outlined in this and related policy documents. All ICT systems users are required to read and accept the contents of this condition of use policy prior to being granted access to ICHAS information systems.

- Documents (hardcopy, online or other media) will be stored in a protected environment for the duration of the Document Retention Schedule set out in the tables below.
- Security of data will be achieved through the implementation of proportionate physical and technical measures.
- The Data Protection Acts (Section 2C (3)) place responsibility for data security squarely on the data controller who is accountable to the individual data subject for the safeguarding of their personal information. A data controller must therefore be satisfied that personal data will be secure including in situations that it is outsourced (e.g. cloud provider).
- Users of the College´s Data Information systems are required to save and store College related data on a protected network location or shared drive and not on personal storage systems.
- Access on Information systems is restricted via the use of passwords and authorised member access levels. Procedures associated with the creation and security of passwords is outlined in further detail below.
- Users wishing to have files, folders or mailboxes in protected locations restored should submit a request to the IS Department.
- The backup of all data is undertaken on a daily basis.
- The Data Protection Officer in conjunction with the QAE officer (or other nominee of the Board of Management) will be responsible for the monitoring and reporting on the effectiveness of the controls.

Retention of Data

- The College will retain data only for as long as necessary, operating a schedule of retention which is set in the tables below for each category of data.
- At least one copy of each document will be retained according to that schedule.
- Hardcopy of documents will be destroyed by shredding after they have been retained until the end of the Document Retention Schedule. Online copies will be destroyed by fire or other proven means to destroy such media after they have been retained until the end of the Document Retention Schedule.
- All data will be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process. In relation to the disposal of any form of personal data, data will only be passed to a disposal partner with demonstrable competence in providing secure disposal service and the nominated 3rd party in this respect for the College is DGD Confidential Shredding Services.
- IT assets holding data will be physically destroyed or degaussed.

Accuracy of Data

- Applications for a change to data should be made in writing to the appropriate programme coordinator.
- Applications for changes to data will receive a response within 14 days of receipt.
- All requests should include:
    - The personal details currently registered with the College to be changed.
    - An outline of the requested change, e.g. changes to surname or address
    - The specific information necessary to process the requested change such as updated name, new address, etc.
    - A summary of the evidence relevant to the application
- Where changes to name or gender are requested, an official legal document, e.g. marriage licence or a statutory declaration, confirming the change, should be provided.
- Students and alumni are advised to notify the College of any changes required to their personal details as soon as possible to ensure all official documentation is produced accurately.
- Upon completion of the change to data, the programme coordinator will inform the subject in writing that the change has been completed.

Procedures associated with the creation and protection of Passwords.

- All users of IS systems are responsible for making sure that the passwords are stored in a secure location to which only the user has access.
- Once a password has been issued to a user, full responsibility for that account and the associated password passes to the user.
- Users must change supplied passwords to user-selected passwords after first login, as directed.
- Under no circumstances are passwords to be revealed to anyone else apart from the authorised user.
- Users must not use any means to obtain another user's password.
- Users must not logon with another user's password.
- Computing devices should not be left unattended without enabling a password-protected screensaver or logging off of the device. All users should lock devices when the device is out of sight.
- Users must not attempt to circumvent password entry with auto logon, application remembering, embedded scripts or hard coded passwords in client software.
- Users must not attempt to gain administrative rights unless granted by IT Admin. Any attempt to gain inappropriate rights is considered a significant breach of the permitted Conditions for Use.
- Strong passwords are essential to the security of the Colleges systems. A strong password is a password that is not easily guessed and advice on generating a strong password will be provided to all users.

Procedures relating to Email Usage

Email is an indispensable tool within the College. College email accounts are provided to all staff and students. The same ethical, legal and commercial standards apply to both internal and external email as to any other form of correspondence. However, limited use of

personal email is permitted subject to the conditions set out in this document and underpinned by the more detailed Security Policies. Standard unencrypted email should never be used to send any data of a personal or confidential nature. Users should secure the information by including it in a password protected document or compressing file or files in a password protected/encrypted zip file. Then provide the recipient with the password by means of other communication, for instance by telephone.

- College data of a personal or confidential nature should never be sent to personal web mail accounts such as (Yahoo, hotmail, gmail etc)
- Non-temporary passwords should never be transmitted by email.

Email Accounts

All accounts maintained on the Colleges email systems are the property of the College. Passwords must not be given to or shared with other people. If access to another email account is required for a business-related reason, the owner of the email account can delegate access or if the owner of the email account is not available, access may be granted on a case-by-case basis on receipt of a business case from the Manager, submitted to the Information systems Manager.

Legal Requirements

The following are required by law and are to be strictly adhered to:

- It is strictly prohibited to send, receive, store or forward emails containing libellous defamatory, offensive, racist, indecent, obscene, or otherwise illegal content. If an email with any of this content comes to the attention of any user that user must promptly notify IS Department.
- Users are reminded that it is also a criminal offence under Irish Law to knowingly infringe intellectual property rights, such as copyrights, patents, database rights and registered trademarks and that sharing copyright material may consequently constitute a criminal offence if done without permission of the right owner in question.
- Users should not forge or attempt to forge email messages.
- Users should not send email messages using another person's email account.
- Users should not disguise or attempt to disguise the user's identity when sending emails.

Personal use of email

Although the College email system is provided for educational purposes, the College also allows the reasonable use of email for personal purposes, if the following conditions are adhered to:

- Personal use of email should not interfere with work.
- Personal emails must comply with the conditions of use set out in this document.
- The use of the College 's emails for registration to non business-related web sites is not recommended. Registration to non business-related web sites could substantially increase the amount of Spam emails both the user and the College receives.

E-mail Attachments

- Users should ensure that only necessary attachments are sent.
- Emails of 10 Megabytes or larger should not normally be sent using the College 's email system. Attempts by standard users to send emails of 10 Megabytes or larger may be blocked, users may contact IS Department for advice on other solutions for transfer of files above 10 Megabytes.

- All sensitive data files should be password protected for transmission. In the case where a password protected file is sent via email, the password should only be communicated via phone call to a nominated person.

Inbound Email Content
The following types of email and content may not be delivered to users:

- Known SPAM
- Unknown Recipient (To) address
- Attachments containing executables such as: .exe, .msi, java and .pif.
- Attachments containing compressed files such as: .tar, .rar, .cab.
- Encrypted attachments
- Attachments containing Multimedia files such as: .mp3, .avi, .wav, .mpeg etc.
- Emails that cannot be scanned by the anti-virus systems.

In such cases, the intended recipient should receive an email to highlight that an intended email to them has been blocked. Users may contact the IS Department and request that the blocked email be released. The IS Department will only release an email, once the team is confident that the email will not cause harm to the College's systems.

Mailbox Size & Email Maintenance
Long-term storage of emails should not result in oversized mailboxes. Emails may be saved to archives by arrangement with the Services Manager. Personal emails should be deleted or archived by users, once they have been read, to help keep the mailboxes size down. The Internet is an indispensable business tool within the College. This facility is provided purely as a business tool. However, limited use of the Internet for personal reasons is permitted subject to the conditions set out in this document.

Procedures relating to Internet Usage
Blocked Web Sites
The College may implement a measure to restrict access to certain categories of web sites. This measure will block certain Internet activities that are deemed unsuitable and/or unacceptable. If access is required to a blocked website for a legitimate business reason, a written request should be submitted by the relevant manager to the IS Department and access may be granted, where appropriate.

Personal Use of the Internet
Although the Colleges systems provide access to the Internet for business use, the College also allows the reasonable use of the Internet for personal purposes, if the following conditions are adhered to.

- Personal use of the Internet must not interfere with work.
- Personal use must comply with the conditions of use set out in this document,
- The College Internet must not be used in support of an external business. For example: the use of Ebay or other auction sites is not allowed for external business purposes.

Monitoring of Internet Usage
The College may monitor Internet usage on the systems. Internet activities may be logged for further review, where necessary, to ensure that users adhere to the conditions for use

set out in this document. Reports on Internet usage may be made available to Management on request.

Web Based Remote Access Software
The use of the Internet to gain remote access to another device either within or external to the College network is generally prohibited. However authorised users may be permitted to use accredited remote access software.

Downloading from the Internet
Downloading of the following file types without approval from the IS Department is prohibited. The IS Department may put measures in place to prevent such files from being downloaded:

- exe - Executable File.
- com - Command File (Executable).
- msi - Windows Installer File (Executable).
- dll - Dynamic Link Library.
- bat Batch File.
- vbs Visual Basic Script.
- cmd Command Shell.

Note: This list will be amended as new risks arise. Exceptions may be applied for staff.
If a user needs blocked software to be downloaded for a legitimate business reason, a request should be submitted by the user to the ITSO. Access may be granted, where appropriate.
Digital audio files should only be downloaded for business purposes.

Publishing to the Internet
All content published to the ICHAS website must be approved by management prior to being published. Data of a sensitive nature must not be published on the College Website.

Anti-Virus
A virus is a piece of self-replicating code, most often a malicious software programme designed to destroy or damage information on computers. Some viruses cause no damage apart from reproducing, but a significant number are specifically designed to cause data loss or to compromise the confidentiality of files by sending copies of them to others.
Potential sources of viruses include shared media such as USB storage devices or CD-ROMs/DVDs, E-Mail (including, but not limited to, files attached to messages), and software or documents copied over networks such as the Internet. A virus infection is almost always costly to the College either because of the loss of data (possibly permanently), or because of staff time spent on investigation/recovery, or because of delays to important work. Furthermore, any viruses spread from the Organisation's network can lead to serious reputation issues for the College as well as possible legal risks/costs. For these reasons the following procedures are required:

- All desktops, laptops and servers must be installed with the College's standard anti-virus software.
- Users are to report any software virus notifications to the College immediately.

- Users must never open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Such attachments should be 'double deleted' immediately, meaning firstly that they should be deleted in the normal way, and secondly that they should then be deleted from the "deleted items" folder as well.
- User must never copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media.
- Users should always scan any devices (CD-ROM's, USB device, floppy disks, etc) prior to access. 'Right-clicking' on the device and selecting "Scan for Virus" achieves this.
- Users should be suspicious of e-mail messages containing links to unknown Web sites. It is possible that the link is a malicious executable (.exe) file disguised as a link. Users should not click on a link received in a message if the user was not expecting a specific link.
- Users must notify the IS Department of any virus infection detection indicated by the Anti-Virus software.

Software Security

Software Copyrights

It is the Colleges policy to respect and adhere to all computer software copyrights and to adhere to the terms of all software licenses, to which the College is a party.

- Approval for the Purchase of Software and Hardware - Users must submit a request for approval to the IS Manager prior to purchasing any software or Hardware for installation on any College systems. The relevant software or hardware will then be evaluated for suitability, with the objective of avoiding any conflict with the College other systems.
- Bar on Software Installation - Non-IT staff are not permitted to install software on College IT Systems. Request for software installation should be submitted to the IS department.

Physical Security of Organisational Laptop/Portable Device

The physical security of any College laptop/portable device is the responsibility of the member of staff to whom the laptop/portable device has been issued. All laptop users are expected to take all reasonable precautions to secure the laptop and its data. All Laptops/portable devices must be in a secure location when not in use.

- Users must take reasonable precautions when using a laptop out of the office.
- Laptops must not be left unattended whilst logged-on.
- Users must never leave a laptop visibly unattended.
- Users should carry and store the laptop in a padded laptop computer bag or strong briefcase to reduce the chance of accidental damage.
- Users should when using a laptop in a public place e.g., on a train, plane, hotel foyer, etc. be aware that information on the laptop screen may be visible to other people in the vicinity.

Encryption

- All laptops/portable devices must have a boot password configured. Personal, sensitive, or confidential data must be encrypted.

Remote Access

The College has an increasing business requirement for mobile working and working from home. Procedures for the conduct of WFH are outlined below. Approval Remote access

connections to the College network will be strictly controlled and only granted on submission of a valid business case and approval by the Vice President.

Access to the IT network from a remote device will only be granted in line with the following criteria:

- Secure encrypted link (e.g., IPSEC or SSL VPN tunnel) with relevant access controls must be used for remote access.
- Consideration should be given to utilise technologies that will provide for the automatic deletion of temporary files which may be stored on remote machines by its operating system.
- Staff must be aware that it is imperative that any wireless technologies/networks used when accessing the College systems must be encrypted to the strongest standard available.
- Only preconfigured devices can connect to the College's network.
- Two methods of authentication must be required when gaining access to the College's network.
- The connecting device must have up to date antivirus software installed.
- Access to areas within the College network must be adequately granted in line with the users' business requirements.
- Remote access must only be granted to specific individuals, generic remote access is strictly prohibited.

Remote Access Monitoring

- The Information Systems department will ensure that all remote access must be monitored and logged.
- The Information Systems department will ensure that all remote access/firewall logs are reviewed on a regular basis.

Remote Access Termination

Remote access will be terminated in the following circumstances:

- Failure to comply with the Conditions of Use of IT Systems Policy.
- Account inactivity for a significant period.
- A change in the user's status e.g., moving departments, retirement or absence. (N.B. It is the account owner/administrator's responsibility to inform the College that the account is no longer required)

Loss or Theft

- If any College IT device is lost or stolen, the user must immediately notify IS (or Police authority if abroad. A copy of the Police report must be provided to the IS Department).
- The IS will inform the Gardaí if required.
- The IS will disable any lost or stolen Mobile email devices, thus removing all data and rendering the device unusable. Mobile phones will be deactivated.

Reissue/Disposal

- Where a device has been damaged or is end of life, it should be returned to the IT team. The IT team must then ensure that all data is cleared off the device prior to re-issue, or disposal.
- Where a Device has been assigned to an individual in the context of a particular post or responsibility, and the individual transfers, the Device must be returned to IT who must ensure that all data is cleared off prior to reissue to the newly assigned officer.

Disposal of equipment

- Any data stored on these devices must also be erased prior to disposal Besides obvious examples, such as servers, computers and laptops, there are a number of other devices that may store personal data, these may include smart phones, digital photocopiers, etc.
- It is the responsibility of the data controller to ensure that all data previously stored on the devices has been removed prior to disposal.
- It is not sufficient to merely format the hard drives of the devices, as data can still be retrieved.
- Dependant on the nature of the data stored, it is recommended that hard drives should be overwritten between three and five times.
- Where the devices are not being recycled / reused the hard drives can either be physically destroyed or degaussed.
- It is important to consider the different types of equipment that may hold personal data. etc.

Physical Security
Physical security safeguards include the following considerations:

- Perimeter security (monitoring of access, office locked and alarmed when not in use);
- Restrictions on access to sensitive areas within the building (such as server rooms);
- Computer location (so that the screen may not be viewed by members of the public);
- Storage of files (files not stored in public areas with access restricted to staff with a need to access particular files)
- Secure disposal of records (effective "wiping" of data stored electronically; secure disposal of paper records).

The Human Factor
No matter what technical or physical controls are placed on a system, the most important security measure is to ensure that staff are aware of their responsibilities. Data Controllers need to consider the following.

- Effective employee training about the risks of data compromise, their role in preventing it and how to respond in the event of problems can be a very effective line of defence.
- Many organisations set security policies and procedures but fail to implement them consistently.
- Controls focusing on individual and organisational accountability and ensuring that policies are carried out are an important part of any system designed to protect personal data.
- Identify essential controls first and ensure that these controls are implemented across the organisation without exception.
- Data controllers must have procedures in place to manage staff turnover, including retrieval of data storage devices and quick removal of access permissions.

Procedures on Outsourced Data Protection & Security
Before considering entrusting personal data to a third party, e.g., a cloud provider, the College must be satisfied that security standards of a very high level are in place. The provider should be able to give assurances on key issues such as:

- Continued access to data by the data controller (backup and disaster recovery measures)
- Prevention of unauthorised access to data (covers both protection against external "hacking" attacks and access by the cloud provider's personnel or by other users of the datacentre)
- Adequate oversight including by means of contract of any sub-processors used.
- Procedures in the event of a data breach (so that the data controller can take necessary measures – see our data breach guidance)
- Right to remove or transfer data (if the data controller wishes either to move the data back under its own direct control or move it to another cloud provider)

The College will satisfy this consideration by way of a detailed technical analysis incorporating an audit of the third-party provider.

Procedures Relating to Marketing
Targeted direct marketing, giving individuals information about the College's provision and services, is a perfectly legitimate activity - provided it respects the individual's right to privacy. Data protection law imposes strict obligations on the use of personal data for direct marketing. The College's procedures relating to same are outlined as follows.

- Individuals may sign up to receive communications from the College related to courses they are interested in. They may request, or be offered, the opportunity to receive such direct marketing following:
- Attendance at an information meeting (whether in-person or online)
- A telephone enquiry about a programme of study
- An email enquiry about a programme of study
- Individuals will not receive such communications without having provided explicit consent to do so.
- Individuals will be given a right to refuse continued such use of their personal data for such purposes both at the time the data is collected (an "opt-out") and on every subsequent marketing message. The "opt-out" right must be free of charge and explicitly communicated.
- Where the College has obtained contact details in the context of an inquiry or through the provision of another service, it may only use these details for direct marketing by electronic mail if the following conditions are met:
    - The service is of a kind similar to that which the user explicitly consented to receive communications or is of a kind similar to that which was previously provided.
    - At the time the College collected user details, the user was given the opportunity to object, in an easy manner and without charge, to their use for marketing purposes.
    - Each time a marketing message is sent, the College provides the user the opportunity to reject to the receipt of further messages.

GRAPHICAL PRESENTATION OF PROCEDURE
The following tables outlines the Data Retention Periods for different categories of Data storage and retention.

Corporate Records

Articles of Association	Permanent
Memorandum of Understanding	Permanent
Board policies	Permanent
Resolutions	Permanent
Board meeting minutes	Permanent
Tax exemption documents	Permanent
Tax or employee identification number designation	Permanent
Annual corporate filings	Permanent

Financial Records

Chart of Accounts	Permanent
Fiscal Policies and Procedures	Permanent
Audits	Permanent
Financial statements	Permanent
General Ledger	Permanent
Check registers/books	7 years
Business expenses documents	7 years
Bank deposit slips	7 years
Cancelled cheques	7 years
Investment records (deposits, earnings, withdrawals)	7 years
Invoices	7 years
Property/asset/equipment inventories	7 years
Petty cash receipts/documents	3 years
Credit card receipts	3 years

Tax Records

Annual tax filing for the organization	Permanent
Payroll registers	Permanent
Filings of fees paid to professionals	7 years
Payroll tax withholdings	7 years
Earnings records	7 years
Payroll tax returns	7 years

Personnel Records

Employee offer letters	Permanent
Confirmation of employment letters	Permanent
Benefits descriptions per employee	Permanent
Pension records	Permanent
Employee resumes and contracts	7 years after termination
Promotions, demotions, letter of reprimand, termination	7 years after termination
Workers' Compensation records	5 years
Salary ranges per job description	5 years

Insurance Records

Property Insurance policy	Permanent
Directors and Officers Insurance policy	Permanent
Workers' Compensation Insurance policy	Permanent
General Liability Insurance policy	Permanent
Insurance claims applications	Permanent
Insurance disbursements / denials	Permanent

Contracts

All insurance contracts	Permanent
Employee contracts	Permanent

Construction contracts	Permanent
Legal correspondence	Permanent
Loan / mortgage contracts	Permanent
Leases / deeds	Permanent
Vendor contracts	7 years
Warranties	7 years

Management Plans and Procedures

Strategic Plans	7 years
Operational Procedures	Permanent
Vendor contacts	7 years
Disaster Recovery Plan	Permanent

Applications Records

Personal data	7 years
Offer/Acceptance records	7 years
Statistical information	Permanent
School data	7 years

Examination Records

Leaving Certificate data	35 years
GCE data	25 years
FETAC data	25 years
Other qualifications data	25 years
HPAT	2 years
GAMSAT	2 years
MSAP	2 years

Scanned Document

Qualifications	2 years
Supplementary Information Forms	1 year
Higher Education Access Route forms	1 year

Course Documentation & Learner Submitted Data

Virtual Classroom Recordings (Synchronous Classes)	End of Relevant Semester
Student Assignment Submissions (Documents)	End of Programme
Student Recorded Assignment Submissions (Video)	End of Programme
Moodle Modules	End of Programme

Linked Policies and Procedures or Statements

Linked Policies	Policy on Data Collection, Usage & Management
Linked Procedures	Procedure Associated with IT Disaster