

Document Name and Version	10.3 Data Management and Retention Policy and Data Retention Schedule
Policy Number	10.3
Policies that Interact with Policy 10.3	10.1 Data Policy; 10.2 Data Protection Processing Principles 10.4 Data Protection Subject Access Request (SAR) Policy; 10.5 Data Breach Policy; 10.6 Webpage Privacy and Cookie Notice; 10.7 Your Right of Access to Personal Information held by IICP College; Policy 11.5 Incorporating Digital Technology into the Curriculum
Approval Body	Board of Directors
Date of Approval	February 2020
Date Policy Comes into Force	25 th January 2021
Date of Next Review	2025
Revisions	Revised 3 rd May 2023 <ul style="list-style-type: none"> • Retention periods updated • Exceptions to disposal actions in Retention Schedule identified and procedure identified • Responsibilities updated to reflect organisational change

1. Preamble.

1.1. IICP College is committed to the proper and effective management of the records it creates, receives, or otherwise processes, in all formats, in the course of all of its operations, in a manner which:

- is transparent, consistent, and accountable;
- meets legal, regulatory, and audit requirements;
- supports the efficient conduct of its business;
- protects the security and integrity of records and data, including Personal Data;
- ensures the preservation of archives documenting its history and development.

1.2. Particular recognition is given to IICP College's obligations as a data controller and processor towards data subjects under the College's Data Protection Policies and Data Protection legislation.

1.3. This policy sets out:

1.3.1. A retention schedule which lists retention periods and disposal instructions for records of IICP College;

1.3.2. Procedures for implementing and auditing the retention schedule;

1.3.3. Arrangements for the preservation of records of permanent value;

1.3.4. Procedures for the timely and secure destruction of records no longer required and not selected for permanent retention.

1.3.5. Exceptions to disposal actions in the Retention Schedule, where disposal action of records may need to be suspended. This may occur, for example, if legal proceedings or an investigation are pending

2. Purpose.

2.1. This policy assigns specific responsibility and introduces procedures for ensuring that files are purged regularly and securely, and that personal data is not retained any longer than is required.

2.2. This policy includes a retention schedule that sets out guidelines for how long IICP College should retain records.

2.3. This policy addresses the following legislative and regulatory requirements:

2.3.1. General Data Protection Regulation [GDPR].

2.3.2. QQI Sector-Specific Quality Assurance Guidelines for Independent/ Private Providers: Management of legislative and regulatory compliance.

3. Scope.

3.1. All employees are responsible and accountable for creating and keeping accurate and complete records of their business activities. Employees must ensure that the records and data for which they are responsible are securely managed in a manner which is compliant with this Policy, and related IICP College policies.

3.2. This Policy applies to all records, in all formats, created, received, maintained or otherwise processed in the course of the activities of IICP College including, without limitation, hard copy and digital records.

3.3. Personal records unrelated to IICP College activities are not within the scope of this policy. Employees are advised to avoid maintaining such records within IICP College systems (eg, email servers, network folders), as doing so may place them within the scope of this and related College policies, and data protection legislation.

4. Roles and Responsibilities.

4.1. The Board of Directors is responsible for formally approving this policy and for overseeing its implementation. The Board is responsible for formally approving the associated Retention Schedule.

4.2. The Executive Management Team has responsibility for overseeing the operation of this policy, including oversight of practices for destruction and archiving data.

4.2.1. Changes to the Retention Schedule

- 4.2.1.1. Changes to the Retention Schedule may be approved by the Executive Management Team, which is responsible for maintaining the master set of the Retention Schedule.
- 4.2.2. Changes may include the addition of new records series, changes to disposal periods, or changes to the final disposal method.
- 4.3. The Data Protection Contact has responsibility for the management of data in accordance with this policy. Specifically, the Data Protection Contact is responsible for:
 - 4.3.1. Developing and maintaining a Data Register for the different areas of operation of the College;
 - 4.3.2. Developing and maintaining a Data Retention plan for each record;
 - 4.3.3. Establishing practices for destruction and archiving data;
 - 4.3.4. Maintaining a record of disposal actions;
 - 4.3.5. Presenting any proposals for change to the Retention Register to the Executive Management Team.
- 4.4. All Users processing records or data created in the course of IICP College's activities must ensure that they do so in a manner that safeguards and protects the integrity, confidentiality and availability of the data at all times. They are expected to acquaint themselves and comply with relevant policies of the College and with all applicable legal requirements, particularly in relation to data protection and copyright. Please contact the Data Protection Contact in the event of any queries.

5. Policy.

- 5.1. IICP College has in place a data retention and destruction policy, which sets out retention and disposal actions and retention periods for College records. Disposal of the vast majority of records occurs at a specified stage of their life-cycle.
- 5.2. Records are retained for as long as they are required by IICP College, and in accordance with legislative, regulatory and audit requirements, and community expectations.

5.3. Exceptions to disposal actions in Retention Schedule (i) current process requiring suspension of disposal:

5.3.1. Where records liable for destruction or deletion are relevant to an ongoing or pending formal process, such as an appeal, an audit, an investigation, a formal information request, or legal proceedings, disposal action must be suspended until that formal process has terminated.

Intentionally destroying or altering a record relevant to such a process may be an offense in law.

5.4. Exceptions to disposal actions in Retention Schedule (ii) Review of records for disposal purposes

5.4.1. Review is chosen as the disposal action for records within a series when it is not clear, at the time of creation, how long they may continue to be of value, or when it becomes clear prior to their disposal that they may continue to be of value, for example, as a result of legislative or regulatory change.

5.4.2. Where records are liable for Review, they must be inspected to determine whether:

5.4.2.1. They are of no further business, legal, audit, or historic value, and so may now be destroyed/deleted;

5.4.2.2. They are of historic value, or of indefinite business value, eg, for precedent purposes, and so may be reclassified as archives;

5.4.2.3. They are still of business, legal, audit, or reference value, and so should be retained for a further retention period and reviewed again thereafter.

5.5. It is important that records are not retained indefinitely 'just in case'. There must be documented reasons for extending retention, signed and approved by relevant staff, as set out in section 6.7 below.

5.6. The general principles of record management are:

5.6.1. Archival documents are protected.

5.6.2. Records that are no longer of value are disposed of, and their destruction occurs at opportune times.

5.6.3. Practical guidelines for the disposal of records or their transfer to the archives are described.

5.6.4. Where the purpose for which personal information was obtained has ceased and the personal information is no longer required, personal data must be deleted or disposed of in a secure manner.

5.7. IICP College has in place a retention schedule which organises records in categories (a record series) that have related legal and operational retention requirements. A retention period or rule is associated with each record class. Exceptions may occur in accordance with section 5.3 or 5.4. All retention schedules will be periodically reviewed in light of experience and any legal or other relevant indications.

6. Procedures.

6.1. The Data Protection Contact, reporting to the Executive Management Team, will ensure the appraisal, disposal, destruction, and archiving of records in accordance with this policy.

6.2. Appraisal:

6.2.1. On an annual basis the Data Protection Contact will carry out a records appraisal for all records held by IICP College.

6.2.2. Appraisal refers to the process of examining and evaluating records in order to determine which records should be kept and for how long, in order to meet the needs of the organisation, legal and regulatory requirements, and the expectations of other users of records.

6.2.3. Appraisal will result in either the disposal of records or their permanent retention as archives.

6.2.4. For the most part, appraisal decisions are governed by the data retention schedules. The schedules should be consulted where decisions on the retention or destruction of records are being taken.

6.3. Disposal:

6.3.1. Disposal should be:

- Authorised;
- Timely;
- Secured;
- Documented.

6.3.2. The destruction of records should be carried out in such a manner that information is irrecoverable. Depending on the format of records, destruction may be affected using different methods.

6.3.3. Sensitive records should be destroyed by secure means, and their disposal documented.

6.4. Disposal procedures:

6.4.1. An important consideration is that material should be disposed of in a manner that befits its sensitivity.

6.4.2. While some records are required to be destroyed in a secure manner, other material does not require this level of security. A distinction should be drawn between material which is genuinely sensitive and that which may be discarded as rubbish. Transient records and drafts may simply be torn up, placed in a litter bin and recycled. This is specifically mentioned for the convenience of staff members. These guidelines specify that sensitive records must be destroyed securely, and where this occurs, destruction must be documented. However, non-sensitive records are discarded more informally.

6.4.3. Where secure shredding is required, then the credentials of the company whose services are engaged for the destruction of records should be examined.

6.4.3.1. It is recommended that certificates of destruction are obtained and inserted in the destruction register adjacent to the relevant list of records.

6.4.4. Different types of electronic media demand specific methods of destruction in order that secure destruction is affected. The Data Protection Officer will

determine the most appropriate method of secure storage and destruction for electronic files.

6.5. *Archive:*

6.5.1. Archives are records created or received and retained by IICP College in the course of conduct of affairs and retained because of continuing value. The overwhelming rationale for careful and documented retention of records and archives is that they may be located for further use.

6.5.2. From time to time archival practices are developed by the Executive Management Team, who oversee their implementation. These practices are subject to change where the activities of the College so require.

6.6. Moodle data:

6.6.1. Moodle is IICP College's Virtual Learning Environment (VLE). It provides one central location for interactions with students, sharing of resources, and management of assignments grading and assessment feedback.

6.6.2. In order to appropriately manage Moodle, and adhere to the College's Data Protection responsibilities, Moodle cannot remain open indefinitely. It is designed as stage specific support for learners and should be available for them for the duration of a given academic year. Learners should note that it is their responsibility to download and save any material that they might want to retain going forward.

6.6.3. Consequently, at the end of the academic year, a phased process of archiving and eventual destruction of that academic year's Moodle data will begin. Learners are provided with adequate information of the deletion process for their cohort to allow them to save and retain their data.

6.6.3.1. Information provision occurs in a number of ways, including:

6.6.3.1.1. Moodle Deletion procedure is included in each handbook for learners.

6.6.3.1.2. At the end of a given academic year, learners receive a closing email for the year. This will include the dates of the Examination Session and the date after which their Moodle data will be deleted.

6.7. Guidance on Review of Records for Disposal Purposes.

6.7.1. Exceptions to disposal actions and retention periods in the Retention Schedule are set out in sections 5.4 and 5.5. In order to determine whether an exception should be made, the following steps must be carried out and documented.

6.7.2. Step 1: Assess the Ongoing Value of the Record

6.7.2.1. Questions to address when assessing value and deciding what to keep on Review should include:

1. Do you still need the records to carry out business in your area? (Eg, files still consulted)
2. Is there a legal or audit requirement to continue to retain the records? (eg, new legislation)
3. Are the records still needed as evidence of how a decision or policy was made? (e.g., if challenged in court, or for public accountability)
4. Are the records of clear and significant precedent value? (eg, for dealing with similar situations in the future which are likely to arise)
5. Are the records needed to protect the legal rights and interests of the College or of individuals?
6. Are the records of research or historical interest?

6.7.2.1.1. If the answer is yes to any of questions 1-3, the file should be retained for further review, to occur at the termination of a second retention period. This second period will generally be the same as the first period as applied under the Schedule, unless new legislation or policy requires longer or permanent retention.

6.7.2.2. If the answer is yes to any of questions 4-6, the files should generally be designated as being of archival value and prepared for transfer to archives.

6.8. Data Retention Schedule: Organisational Records

HR Records	Retention Period	Rationale	Final disposition
Unsolicited applications for positions	None.	There is no requirement to retain unsolicited records. Under the principle of data minimisation, IICP College does not retain records of unsolicited applications for jobs.	Confidential shredding / secure deletion of electronic records
Vacancy notification, Advert copies, Job description, Selection criteria.	Until original vacancy is superseded.	To facilitate reviews of organisational structures. To enable a smooth transition where a post/ posts change in terms of roles and responsibilities.	Confidential shredding / secure deletion of electronic records
Candidates not qualified or short listed for interview: Cover letters, application forms/CVs etc. Applications and CVs of candidates shortlisted for interview but who do not attend: Cover letters, application forms/CVs etc. Candidates short listed and who attend interview but who are not successful or who are successful but do not accept offer: Cover letters, application forms/CVs etc.	Retain until final appointment has been approved plus 1 year	Under Employment Equality Legislation a candidate/ employee who believes they have suffered discrimination on one of the nine grounds can refer a case to the Equality Tribunal for	Confidential shredding / secure deletion of electronic records

		investigation within 6 month of last alleged act.	
Interview Board marking sheet, interview Board notes, recommendation by Interview Board	Retain until final appointment has been approved plus 1 year	Under Employment Equality Legislation a candidate/ employee who believes they have suffered discrimination on one of the nine grounds can refer a case to the Equality Tribunal for investigation within 6 month of last alleged act.	Confidential shredding / secure deletion of electronic records
Payroll Pay-sheets, authorisations to deduct, tax details of staff, appointment details, pay scales	Retain on personnel file for duration of employment and for 6 years after termination of employment	Finance Act 2020	Confidential shredding /secure deletion of electronic files
In relation to each employee: <ul style="list-style-type: none"> • Annual Leave and Public Holiday records • Total days and hours worked in each week • Any days and hours of leave taken each week (including annual leave and public holidays), and the payment for that leave • Any additional pay for a public holiday 	Retain on personnel file for 3 years	This is required by the Organisation of Working Time Act, 1997, section 25	Confidential shredding /secure deletion of electronic files

Employment Permit records	5 years of for the duration of the employment (whichever is the longer)		Confidential shredding /secure deletion of electronic files
PPS numbers, Payslips and records relating to wages	Retain on personnel file for 3 years following termination of employment	This is required by the Organisation of Working Time Act, 1997, section 25	Confidential shredding /secure deletion of electronic files
Contracts of Employment	Retain for 7 years post termination of the contract	Business use	Confidential shredding /secure deletion of electronic files
Parental/paternity/force majeure/maternity/adoptive/carer's leave	8 Years.	Parental Leave Acts 1998-2007 provide for an 8 year retention period.	
Personnel Files. These may contain: <ul style="list-style-type: none"> • Personal contact details • Application form/CV/cover letter • Contract of employment (offer of appointment, date appointed) • Evidence of education qualifications • References • Questionnaire on criminal offences • Recruitment medical • Probation forms • Salary rates and increments • Service records • Record of mandatory training (where relevant) • Termination notices 	Retain on personnel file for duration of employment and for 5 years after last pension payment	Business use	Confidential shredding /secure deletion of electronic files

<ul style="list-style-type: none"> • Training and development records • Safety training records • Occupational health reports • , 			
<p>Discipline records Records relating to disciplinary actions taken against employees e.g. warnings, suspensions recorded, or copy warnings placed on an employee's personnel record etc.</p>	<p>Hold on personal file/disciplinary file for duration of employment plus 7 years after resignation/retirement, then destroy. Where disciplinary policy provides for earlier removal then destroy but keep a record that a warning was issued. Where the matter involved criminal activity these records should be retained indefinitely.</p>	<p>No longer needed 7 years after employment ends.</p>	<p>Confidential shredding /secure deletion of electronic files</p>
<p>HR allegations and complaints Written allegations/ complaints: records received/created as a result of investigating allegations / complaints</p>	<p>Where the complaint is found to be untrue or unwarranted make a note on personal file index that a complaint was made, but there is no need to keep detailed documentation or refer back to previous cases if further separate allegations are made in the future.</p>	<p>Retaining details of unfounded complaints beyond the conclusion of the investigation process could create a legal liability for the College</p>	<p>Confidential shredding /secure deletion of electronic files</p>

Health and Safety Records	Retention Period	Rationale	Final disposition
Safety policies	Retain for 2 years after superseded then destroy	Safety, Health and Welfare at Work legislation	Shredding
Risk assessments records	Retain for 5 years after superseded then destroy	Business use	Confidential shredding /secure deletion of electronic files
Fire drill records	Retain for 5 years	Business use	Shredding

Incident reports e.g. Accident reports and dangerous occurrence report forms	Retain for 10 years after date of incident	Safety, Health and Welfare at Work legislation	Confidential shredding /secure deletion of electronic files
Personal injuries:	3 years from the date of the injury (subject to H&S instances which may necessitate a 10 year retention period)	Business use	
Notifications of personal accidents	Refer to insurance	Business use	Confidential shredding /secure deletion of electronic files

OTHER	Retention Period	Rationale	Final disposition
Legal records	Retain indefinitely		Appropriate filing / secure archiving
Tax records	6 years (not in respect of an open revenue case) 6 years after closure of a revenue case		Confidential shredding /secure deletion of electronic files

7.2 Data retention Schedule: Academic Records.

Learner Records	Retention Period	Rationale	Final disposition
Admissions Records of successful direct entry applicants	Retain for duration of studies plus up to 3 years	Required for Programme Review purposes	Confidential shredding / secure deletion of electronic records
Records of unsuccessful applicants (undergraduate & postgraduate) where no appeal initiated	Retain for up to 5 years.	Required for Programme Review purposes	Confidential shredding / secure deletion of electronic records
Unsuccessful applicant appeals submissions, Appeal committee reports/outcomes	Retain for up to 5 years following completion of action	Required for Programme Review purposes	Confidential shredding / secure deletion of electronic records
Learner Record detailing:	Retain indefinitely	Part of College academic record.	Appropriate filing / archiving

<ul style="list-style-type: none"> • Student name • Student number • Contact details • Date(s) of registration • Courses/ modules taken • Results of examinations/ assessments • Dates of graduation/ withdrawal from IICP College 			
<p>Records including: Mitigation / extenuating circumstances forms, requests for extensions, leave of absence, deferral, transfer, readmission, exemptions. Records relating to access, disability, references, medical/ sick certificates and work placements</p>	Retain for duration of studies plus up to 1 year	May have relevance to student's assessment.	Confidential shredding / secure deletion of electronic records
General correspondence with students.	Retain until matters raised are actioned or queried.	Data minimisation: no longer needed after that.	Confidential shredding / secure deletion of electronic records
Attendance records	Retain for duration of studies plus 1 year	May have relevance to student's assessment.	Confidential shredding / secure deletion of electronic records
Learner fees/ financial: Recorders learner fees, payment records, bank giros	Retain for duration of studies plus up to 3 years	Business use	Confidential shredding / secure deletion of electronic records
Academic progress records, including: records re supervision and support not held centrally in Academic Registry	Retain for duration of studies plus up to 3 years	May have relevance to student's assessment.	Confidential shredding / secure deletion of electronic records

<p>Discipline records Records relating to disciplinary actions taken against learners</p>	<p>Where not upheld, then destroy. Where upheld, hold on personal file/disciplinary file for duration of studies plus 7 years and then review. Where disciplinary policy provides for earlier removal then destroy but keep a record that a warning was issued. Where the matter involved criminal activity these records should be retained indefinitely.</p>	<p>Data minimisation: no longer needed after that. May have relevance to student's progression.</p>	<p>Confidential shredding /secure deletion of electronic files</p>
<p>Complaints records. Written allegations/ complaints: records received/created as a result of investigating allegations / complaints</p>	<p>Where the complaint is found to be unwarranted make a note on personal file index that a complaint was made, but there is no need to keep detailed documentation or refer back to previous cases if further separate allegations are made in the future. Where upheld, maintain for duration of studies plus 7 years, then review.</p>	<p>Retaining details of unfounded complaints beyond the conclusion of the investigation process could create a legal liability for the College</p>	<p>Confidential shredding /secure deletion of electronic files</p>

Garda Vetting records:	Retain for duration of study plus 3 yrs.	May have relevance to student's progression.	Confidential shredding /secure deletion of electronic files
Examination, results, graduation records			
Examination / Assessment papers, Assessment briefs and related records	Retain for one year and then review	Part of College record.	Confidential shredding /secure deletion of electronic files
Records which contribute towards module grade such as essays, case studies (These have been returned to learners)	Retain for duration of study plus grace period notified to students (see section 6.6)	These have relevance to student's assessment and may be required for an appeal.	Confidential shredding /secure deletion of electronic files
Final Year undergraduate Projects/ Dissertations and associated records, raw data, supervision records etc.	Retain for duration of study plus grace period notified to students (see section 6.6)	These have relevance to student's assessment and may be required for an appeal.	Confidential shredding /secure deletion of electronic files
Postgraduate theses	Retain indefinitely	QQI requirement (Assessment and Standards 2013)	Appropriate storage / archiving
Assessment scripts which undergo recheck / appeals procedures. 1. Original script 2. Examinations Recheck and Appeal form, outcome record	1. Retain for up to 2 years after action completed 2. Retain indefinitely	These have relevance to student's assessment and may be required for further proceedings. May be required in College reviews.	Confidential shredding /secure deletion of electronic files Appropriate filing / secure archiving
External examiners' reports	Indefinitely.	Part of College Records	Confidential shredding /secure deletion of electronic files
External Examiners correspondence, meetings records etc.	Retain for a period of current year plus 5 years, or completion of	May be required in College reviews.	Confidential shredding /secure deletion of electronic files

	next revalidation, whichever is the longer		
Records of module marks and amendment to marks, Formal broadsheets, Examination board meeting records, Learner academic transcript, Diploma Supplement	Retain indefinitely	Part of College record. Required by QQI	Appropriate filing / secure archiving
Records of applicants for and attendees at Taster events.	None	Applicant personal data is required to facilitate remote attendance at Taster events. There is no requirement to retain these records beyond the Taster event. Under the principle of data minimisation, IICP College does not retain records of applicants and attendees at taster events	Confidential shredding /secure deletion of electronic files
Alumni records	For as long as each individual alumnus consents to be contactable	To facilitate communication between IICP College and its alumni community.	

General Academic Records	Retention Period	Rationale	Final disposition
IICP College policies and procedures	Indefinitely.	Part of College record.	Confidential shredding / secure deletion of electronic records
Strategic Plans (including Teaching and Learning, Access Transfer and Progression)	Indefinitely.	Part of College record.	Non-secure Shredding / Recycling Archive (non-secure)
Records of Board & Academic Council	Indefinitely.	Part of College record.	Confidential shredding / secure

and their Committees (Minutes, etc.)			deletion of electronic records
Records of hearings, (e.g. Appeals boards etc.)	Retain in accordance with policy, Otherwise, retain for 5 years after relevant action completed	These records are required for QOI reviews.	Confidential shredding /secure deletion of electronic files Appropriate filing / secure archiving
Routine administration records	Retain for current year, or until they cease to be of administrative use	Data minimisation: no longer needed after that.	Appraise and evaluate for secure archiving where relevant otherwise, confidential shredding / secure G deletion of electronic records
Quality reports, quality assurance peer reviews	Indefinitely.	Part of College record.	Confidential shredding /secure deletion of electronic files
Correspondence with accreditation bodies etc.	Indefinitely.	Part of College record.	Appropriate filing / secure archiving
Teaching allocations/semester schedules	Retain until superseded plus up to 2 years.	Part of College record.	Confidential shredding /secure deletion of electronic files
Marketing Material	Retain until superseded plus up to 2 years.	Part of College record.	Non-secure Shredding / Recycling Archive (non-secure)
Legal records	Retain indefinitely	Part of College record.	Appropriate filing / secure archiving

Please note that in certain circumstances, we may hold your data for a longer period, for example, if we are processing an ongoing claim or believe in good faith that the law or a relevant regulator may reasonably in our view expect or require us to preserve your personal data