CITY OF WOLVERHAMPTON COLLEGE

Data Retention & Erasure

Policy and Procedure 2026-27

GDPR Manager

Publication: August 2018 | Version No. 1.0

Review: August 2026

1.0. Policy Statement

1.1. City of Wolverhampton College recognises that the efficient management of its data and records is necessary to support its core business functions, to comply with its legal, statutory and regulatory obligations, to ensure the protection of personal information and to enable the effective management of the organisation.

1.2. This policy and related documents meet the standards and expectations set out by contractual and legal requirements and has been developed to meet the best practices of college records management, with the aim of ensuring a structured approach to document control.

1.3. **Effective and adequate records and data management is necessary to:**

- Ensure that the College conducts itself in a structured, efficient and accountable manner
- Ensure that the College realises best value through improvements in the quality and flow of information and greater coordination of records and storage systems
- Support core business functions and provide evidence of conduct and the appropriate maintenance of systems, tools, resources and processes
- Meet legislative, statutory and regulatory requirements
- Deliver services to, and protect the interests of, employees (prospective, Current and ex-members), students (prospective, current and historical), clients and stakeholders in a consistent and equitable manner
- Assist in document policy formation and managerial decision making
- Provide continuity in the event of a disaster or security breach
- Protection personal information and data subject rights
- Avoid inaccurate or misleading data and minimise risks to personal information
- Erase data in accordance with the legislative and regulatory requirements

1.4. Information held for longer than is necessary carries additional risk and cost and can breach data protection rules and principles. The College only ever retains records and information for legitimate or legal business reasons and always comply fully with the data protection laws, guidance and best practice.

2.0. Purpose

2.1. The purpose of this document is to provide the College's statement of intent on how it provides a structured and compliant data and records management system. We define ***'records'*** as all documents, regardless of the format; which facilitate business activities and are thereafter retained to provide evidence of transactions and functions in support of audit and similar activities.

2.2. Such records may be created, received or maintained in hard copy or in an electronic format with the overall definition of records management being a field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use, distribution, storage and disposal of records.

3.0. Scope

3.1. This policy applies to all staff within the College *(meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the College).* Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

4.0. Personal Information and Data Protection

4.1. The College needs to collect personal information about students and the people we employ, work with / have a business relationship with, to effectively and compliantly carry out our everyday business functions and activities, and to provide educational products and services. This information can include *(but is not limited to),* name, address, email address, data of birth, IP address, identification number, private and confidential information, sensitive (special category) information and bank details.

4.2. In addition, we may occasionally be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations, however we are committed to collecting, processing, storing and destroying all information in accordance with the ***General Data Protection Regulation UK GDPR 2018***, current UK data protection legislation and any other associated legal or regulatory body rules or codes of conduct that apply to our business and/or the information we process and store.

4.3. **Our Data Retention Policy and processes comply fully with the UK GDPR's Article 5 principle:**

- 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')

5.0. Objectives

5.1. A record is information, regardless of media, created, received, and maintained which evidences the development of, and compliance with, regulatory requirements, business practices, legal policies, financial transactions, administrative activities, business decisions or agreed actions. It is the College's objective to implement the necessary records management procedures and systems which assess and manage the following processes:

- The creation and capture of records
- Compliance with legal, regulatory and contractual requirements
- The storage of records

- The protection of record integrity and authenticity
- The use of records and the information contained therein
- The security of records
- Access to and disposal of records

5.2. Records contain information that are a unique and invaluable resource to the College and are an important operational asset. A systematic approach to the management of our records is essential to protect and preserve the information contained in them, as well as the individuals such information refers to. Records are also pivotal in the documentation and evidence of all business functions and activities in an audit scenario.

5.3. ***The College's objectives and principles in relation to Data Retention are to:***

- Ensure that the College conducts itself in an orderly, efficient and accountable manner
- Support core business functions and providing evidence of compliant retention, erasure and destruction
- To develop and maintain an effective and adequate records management program to ensure effective archiving, review and destruction of information
- To only retain personal information for as long as is necessary
- Comply with the relevant data protection regulation, legislation and any contractual obligations
- Ensure the safe and secure disposal of confidential data and information assets
- Ensure that records and documents are retained for the legal, contractual and regulatory period stated in accordance with each body's rules or terms.
- Ensure that no document is retained for longer than is legally or contractually allowed
- Mitigate against risks or breaches in relation to confidential information

6.0. Guidelines & Procedures

6.1. The College manage records efficiently and systematically, in a manner consistent with the GDPR requirements and current UK legislative requirements. Records management training is mandatory for all staff as part of the College's statutory and compliance training programme and this policy is widely disseminated to ensure a standardised approach to data retention and records management.

6.2. Records will be created, maintained and retained to provide information about, and evidence of the College's student, employment and customer activities. Retention schedules will govern the period that records will be retained and can be found in the Information Asset Register

6.3. **It is our intention to ensure that all records and the information contained therein is:**

- **Accurate** - records are always reviewed to ensure that they are a full and accurate representation of the transactions, activities or practices that they document
- **Accessible** - records are always made available and accessible when required (*with additional security permissions for select staff where applicable to the document content*)
- **Complete** - records have the content, context and structure required to allow the reconstruction of the activities, practices and transactions that they document
- **Compliant** - records always comply with any record keeping legal and regulatory requirements
- **Accountable** – clear ownership is assigned for records throughout their lifecycle. Information Asset Owners, managers and staff are responsible for ensuring that records are created, maintained, retained, reviewed and securely disposed of in accordance with this Policy and applicable legal and regulatory requirements.
- **Monitored** – staff, college and system compliance with this Data Retention Policy is regularly monitored to ensure that the objectives and principles are being complied with at all times and that all legal and regulatory requirements are being adhered to.

7.0. Retention Period Protocols

7.1. All records retained during their specified periods are traceable and retrievable. All College, student and employee information is retained, stored and destroyed in line with legislative and regulatory guidelines.

7.2. **For all data and records obtained, used and stored within the College, we:**

- Carry out periodical reviews of the data retained, checking purpose, continued validity, accuracy and requirement to retain
- Establish periodical reviews of data retained
- Establish and verify retention periods for the data, with special consideration given in the below areas:
    - the requirements of the College
    - the type of personal data
    - the purpose of processing
    - lawful basis for processing
    - the categories of data subjects

7.3. Where it is not possible to define a statutory or legal retention period, as per the UK GDPR requirement, the College will identify the criteria “Best Practice” by which the period can be determined and provide this to the data subject on request and as part of our standard information disclosures and privacy notices.

7.4. Have processes in place to ensure that records pending audit (with reference to the requirements of European Social Fund match funding and related retention periods), litigation or investigation are not destroyed or altered.

7.5. Transfer paper-based records and data to an alternative media format in instances of long retention periods (with the lifespan of the media and the ability to migrate data where necessary always being considered).

8.0. Designated Owners

8.1. All systems and records have designated owners (IAO) throughout their lifecycle to ensure accountability and a tiered approach to data retention and destruction. Owners are assigned based on role, college area and level of access to the data required. The designated owner is recorded on the Information Asset Register and is fully accessible to all employees.

9.0. Document Classification

9.1. The College utilises an *Information Asset Register (IAR)* to document and categorise the assets under our remit and carry out regular Information Audits to identify, review and document all flow of data within the College.

9.2. We also carry out regular Information Audits to identify, categorise, map, and review all personal data obtained, processed, stored, shared, and disposed of by the College in its capacity as both a data controller and, where applicable, a data processor. The findings of these audits are maintained within the College's Information Asset Register (IAR), providing an auditable record of our processing activities and supporting our accountability obligations under Article 5(2) and Article 30 of the UK GDPR. The register includes, but is not limited to:

- The information asset name and description
- The categories of personal data held
- Special category and criminal offence data processed (where applicable)
- The categories of data subjects
- The purpose(s) of processing
- The lawful basis for processing
- The source of the personal data
- Who the information is shared with, including third-party processors and recipients
- The location and format of the data (electronic, paper, cloud, etc.)
- The Information Asset Owner (IAO) and responsible department
- Retention and disposal periods
- Access levels and security classifications (e.g., public, internal, confidential, restricted)
- Technical and organisational security measures applied
- Whether a Data Protection Impact Assessment (DPIA) is required or completed

- International data transfers (where applicable)
- Associated risks, controls and mitigation measures
- Review dates and audit outcomes

9.3. Our Information Audits and Information Asset Register enable the College to demonstrate accountability, maintain oversight of personal data processing activities, support compliance with UK GDPR and the Data Protection Act 2018, and ensure that personal information is managed securely throughout its lifecycle.

9.4. **We utilise 3 main classification types:**

a) **Public** - information that is freely obtained from / available to the public and as such, is not classified as being personal or confidential

b) **Protect-** information or a system that processes information that belongs to an individual and is classed as personal under the data protection laws

c) **Confidential** – special category and information deemed sensitive (e.g. medical conditions, disciplinary records etc) that must be secured at the highest level and are afforded access restrictions and high user authentication

9.3. The classification is used to decide what access restriction needs to be applied, and the level of protection afforded to the record or data. The classification along with the asset type, content and description are then used to assess the risk level associated with the information and mitigating action can then be applied.

10.0. Suspension of Record Disposal for Litigation or Claims

10.1. If the College is served with any legal request for records or information, any employee becomes the subject of an audit or investigation or we are notified of the commencement of any litigation against the College, we will suspend the disposal of any scheduled records until we are able to determine the requirement for any such records as part of a legal requirement.

11.0. Storage & Access of Records and Data

11.1. Documents such as enrolment forms, employee records, registers, learner progress monitoring where in a paper-based format, are grouped together by category and then in clear date order when stored and/or archived.

12.0. Expiration of Retention Period

12.1. Once a record or data has reached its designated retention period date, the designated owner should take the appropriate action. Not all data or records are expected to be deleted upon expiration; sometimes it is sufficient to anonymise the data in accordance with the GDPR / current data protection legislative requirements or to archive records for a further period.

13.0. Destruction and Disposal of Records & Data

13.1. All information of a confidential or sensitive nature on paper, card, or electronic media must be securely destroyed when it is no longer required. This ensures compliance with the Data Protection laws and the duty of confidentiality we owe to our employees, students and customers.

13.2. The College is committed to the secure and safe disposal of any confidential waste and information assets in accordance with our contractual and legal obligations and that we do so in an ethical and compliant manner. We confirm that our approach and procedures comply with the laws and provisions made in the General Data Protection Regulation (UK GDPR 2018) / current data protection legislation, and that staff are trained and advised accordingly on the procedures and controls in place.

14.0. Paper Records

14.1. Due to the nature of our business, the College retains paper based personal information and as such, has a duty to ensure that it is disposed of in a secure, confidential and compliant manner. The Co utilise secure confidential waste collection receptacles and contracted on-site shredding services to dispose of all paper materials.

14.2. Employee confidential waste collection points are made available throughout the college campuses and where we use a service provider for large disposals, regular collections take place to ensure that confidential data is disposed of appropriately.

15.0. Electronic & IT Records and Systems

15.1. The College uses numerous systems, computers and technology equipment in the running of our business. From time to time, such assets must be disposed of and due to the information held on these whilst they are active, this disposal is handled in an ethical and secure manner.

15.2. The deletion of electronic records must be organised in conjunction with the ICT Services Department who will ensure the removal of all data from the medium so that it cannot be reconstructed. When records or data files are identified for disposal, their details must be provided to the designated owner to maintain an effective and up to date a register of destroyed records.

15.3. Only the ICT Services Department can authorise the disposal of any IT equipment and they must accept and authorise such assets from the department personally. Where possible, information is wiped from the equipment through use of software and formatting, however this can still leave imprints or personal information that is accessible and so we also comply with the secure disposal of all assets.

15.4. In all disposal instances, the ICT Services Department must complete a disposal form and confirm successful deletion and destruction of each asset. This must also include a valid certificate of disposal from the service provider removing the formatted or shredded asset. Once disposal has occurred, the ICT Services Department is

responsible for liaising with the information Asset Owner and updating the Information Asset Register for the asset that has been removed.

16.0. Internal Correspondence and General Memoranda

16.1. All information held under a staff account that has been closed down will be deleted from the College e-mail system and file store after the period for staff information agreed in the retention schedule from when the account was closed. All student information will be deleted from the College e-mail system after the period agreed in the retention schedule from when the account was closed. There will be no ability to recover information once deletion has been carried out.

16.2. ***Examples of correspondence and memoranda include (but are not limited to):***

- Internal emails
- Meeting notes and agendas
- General inquiries and replies
- Letter, notes or emails of inconsequential subject matter

17.0. Erasure

17.1. In certain circumstances, data subjects have the right to request the erasure of their personal data, commonly referred to as the “right to be forgotten” under Article 17 of the UK GDPR. However, this right is not absolute and must be balanced against the College’s legal, regulatory, contractual, and public task obligations.

17.2. The College will consider requests for erasure where one or more of the following conditions apply:

- The personal data is no longer necessary for the purpose(s) for which it was originally collected or processed.
- The data subject withdraws consent and there is no other lawful basis for continuing the processing.
- The data subject objects to the processing and there are no overriding legitimate grounds for the continued processing.
- The personal data has been processed unlawfully.
- The personal data must be erased to comply with a legal obligation under UK law.
- The personal data was collected in relation to the offer of information society services to a child.

17.3. Where one of the above conditions applies and the College received a request to erase data, we first ensure that no other legal obligation or legitimate interest applies. If we are confident that the data subject has the right to have their data erased, this is carried out by the Data Protection Officer in conjunction with any department manager and the ICT Services team to ensure that all data relating to that individual has been erased.

17.4. These measures enable us to comply with a data subjects right to erasure, whereby an individual can request the deletion or removal of personal data where there is no compelling reason for its continued processing. Whilst our standard procedures

already remove data that is no longer necessary, we still follow a dedicated process for erasure requests to ensure that all rights are complied with and that no data has been retained for longer than is needed.

17.5. The right to erasure does not apply where the College is required to retain personal data for compliance with a legal obligation, the performance of a task carried out in the public interest, the establishment, exercise or defence of legal claims, safeguarding obligations, statutory education requirements, funding regulations, audit requirements, or for archiving purposes in the public interest.

17.6. Upon receipt of an erasure request, the College will:

- Record the request in the Erasure Request Register.
- Verify the identity of the requester.
- Assess whether the request meets the requirements of Article 17 UK GDPR.
- Identify any legal, regulatory, contractual, or public task obligations requiring continued retention.
- Where erasure is approved, securely erase or anonymise the relevant personal data without undue delay and within one calendar month unless an extension is permitted under data protection law.
- Inform the requester of the outcome and, where applicable, notify any third parties with whom the data has been shared, unless this proves impossible or involves disproportionate effort.

17.7. Where the College refuses an erasure request, the data subject will be informed in writing of the reasons for the refusal, their right to request a review, and their right to lodge a complaint with the Information Commissioner's Office (ICO). ***Such refusals to erase data include:***

- Exercising the right of freedom of expression and information
- Compliance with a legal obligation for the performance of a task carried out in the public interest
- For reasons of public interest in the area of public health
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing
- For the establishment, exercise or defence of legal claims

17.8. The College will maintain a record of all erasure requests, decisions, actions taken, and associated correspondence to demonstrate compliance with its accountability obligations under Article 5(2) UK GDPR.

18.0. Special Category Data

18.1. In accordance with GDPR requirements and current UK GDPR legislation and Schedule 1 Part 4 of The Data Protection Bill, organisations are required to have and maintain appropriate policy documents and safeguarding measures for the retention and erasure of special categories of personal data and criminal convictions etc.

18.2. Our methods and measures for destroying and erasing data are noted in this policy and apply to all forms of records and personal data, as noted on our retention register schedule.

19.0. Compliance and Monitoring

19.1. The College is committed to ensuring the continued compliance with this policy and any associated legislation and undertake regular audits and monitoring of our records, their management, archiving and retention. Information asset owners are tasked with ensuring the continued compliance and review of records and data within their remit.

20.0. Responsibilities

20.1. Heads of departments and information asset owners have overall responsibility for the management of records and data generated by their departments' activities, namely, to ensure that the records created, received and controlled within the purview of their department, and the systems (*electronic or otherwise*) and procedures they adopt, are managed in a way which meets the aims of this policy.

20.2. The Data Protection Officer will be involved in any data retention processes and records or all archiving and destructions must be retained. Individual employees must ensure that the records for which they are responsible are complete and accurate records of their activities, and that they are maintained and disposed of in accordance with the College's protocols.

21.0. Retention Periods

21.1. Section 12 of this policy contains our regulatory, statutory and business retention periods and the subsequent actions upon reaching those dates. Where no defined or legal period exists for a record, the default standard retention period is 6 years plus the current year (*referred to as 6 years + 1).*

21.0. Retention Schedule

Area of College	Record	Reason (Regulations or Legislative Act)	Period of Retention	Comment	Responsibility (EMT) & formal responsibility for disposal.	Operational Responsibility
Finance	Financial records (all records including invoices, receipts, copies of ledgers and accounts – electronic and hard copy)		6 years +1		**Deputy Principal and Chief Executive**	**Finance Manager**
	Income tax and NI returns	Income Tax Act 2007	6 years +1			
	Internal and External Audit reports	Good Practice	6 years +1			
	Commercial Contracts	Good Practice	6 years +1			
	Service Contracts	Good Practice	6 years +1			
	Tenders – opening record and evaluation process and tender award contract.	Good Practice	6 years +1			
	Bids, funding / grant applications and returns	Good Practice	As per the requirements of the funder			
Capital Schemes &	Original contractual paperwork including contracts, specifications, maps, drawings etc	Good Practice	Indefinitely		**Deputy Principal and**	

Area of College	Record	Reason (Regulations or Legislative Act)	Period of Retention	Comment	Responsibility (EMT) & formal responsibility for disposal.	Operational Responsibility
Major building projects	All other formal documentation relating to the capital scheme	Good Practice			**Chief Executive**	**Estates Manager**
HR	Personnel files (including notes of formal hearings)	1980 c58 Limitation Act	6 years +1	From end of employment	**Deputy Principal and Chief Executive**	**HR Manager**
	Payroll records (wages & salaries)	Taxes Management Act 1970	6 years +1	From end of employment		**Payroll Manager**
	Statutory Maternity Pay records	Maternity Pay and Statutory Sick Pay Regulations 2002	6 years +1	From end of employment		**Payroll Manager**
HR & Payroll	Statutory Sick Pay records	Maternity Pay and Statutory Sick Pay Regulations 2002	6 years +1	From end of employment		**Payroll Manager**
	Pension records	1980 c 58 Limitation Act	Until staff member becomes pension beneficiary.	Where we pay individuals pension – 12 months		**HR Manager** **HR Manager**

Area of College	Record	Reason (Regulations or Legislative Act)	Period of Retention	Comment	Responsibility (EMT) & formal responsibility for disposal.	Operational Responsibility
HR & Payroll				after this ceases	**Deputy Principal and Chief Executive**	**HR Manager**
	Application forms / interview notes – unsuccessful applicants.	Equality Act 2010	12 months	from application date		
	Application forms / interview notes – successful applicants	Good Practice	6 years +1	From end of employment		**Payroll Manager**
	Personal Redundancy documentation	Litigation	6 years + 1	from end of employment		**Payroll Manager**
	Sickness/health records	Good Practice	6 years +1	after termination of employment. 40-60 years if H&S/Equality Act potential claims		**Payroll Manager**
	Staff training records CPD Records	Good Practice	6 years +1 5 years	From end of employment		**Payroll Manager**

Area of College	Record	Reason (Regulations or Legislative Act)	Period of Retention	Comment	Responsibility (EMT) & formal responsibility for disposal.	Operational Responsibility
				From date of record		
	Pension Records	Limitations Act 1980	1 year	After the last payment of pension		
	DBS disclosure forms	Ofsted requirement	3 years unless the individual is on the update service and the original source document needs to be retained	Individual records 6 + 1 years following termination		
	Single Central Record	Good Practice	Current staff only			
Safety, Health, Fire and Environment	Insurance records	Good Practice	10 years		**Deputy Principal and Chief Executive**	**Safety, Health, Fire and Environment Manager**
	Health Surveillance/Health Records	Limitations Act 1980 Health and Safety at Work Act 1974	60 years	Following termination of employment		
	Medical records kept by reason of COSHH regulations	Limitations Act 1980 Health and Safety at Work Act 1974	60 years			

Area of College	Record	Reason (Regulations or Legislative Act)	Period of Retention	Comment	Responsibility (EMT) & formal responsibility for disposal.	Operational Responsibility
	Risk Assessments – Audits Reports	Health and Safety at Work Act 1974	4 years			
	PAT testing records	Health and Safety at Work Act 1974	4 years			
	Air Monitoring	Health and Safety at Work Act 1974	5 Years			
	Examination and test local exhaust ventilation	Health and Safety at Work Act 1974	5 years			
Safety, Health, Fire and Environment	Accident Register, records and reports of accidents		4 years accident reports RIDDOR reports with HSE		**Deputy Principal and Chief Executive**	**Health & Safety Manager**
Information Systems	Student MIS records (electronic and hard copy)	Good Practice	6 years +1 Unless ESF related, in which case: For enrolments between calendar years 2007 and 2013, records retained until		**Deputy Principal and Chief Executive**	**Funding and Compliance Manager**
	Exam and Assessment records	Good Practice				
	Registers	Good Practice				

Area of College	Record	Reason (Regulations or Legislative Act)	Period of Retention	Comment	Responsibility (EMT) & formal responsibility for disposal.	Operational Responsibility
			at least 31/12/2022 For enrolments between calendar years 2014 and 2020, records retained until at least 31/12/2030		**Deputy Principal and Chief Executive**	**Funding and Compliance Manager**
	Timetables	Good Practice	1 year +1			
IT Services	Software licenses and hardware registers	Good Practice	5 years +1	After expiry of license	**Deputy Principal and Chief Executive**	**ICT Services Manager**
	Residual electronic data (including e-mails and any data held electronically which does not fall into any other category noted)	Good Practice	6 months			
	Access Fund records (HE)	Good Practice	3 years +1			

Area of College	Record	Reason (Regulations or Legislative Act)	Period of Retention	Comment	Responsibility (EMT) & formal responsibility for disposal.	Operational Responsibility
Student Services				After course ends	**Deputy Principal – Student Engagement**	**Head of Student Entitlement**
	Educational Maintenance Allowance records	Good Practice				
	Admissions records	Good Practice				
	Confidential student files (Tutor Assistants)	Good Practice				
	Confidential student counselling records	Good Practice				
	Careers Action Plans / forms	Good Practice	3 years +1	after course ends (May need to be longer if Equality Act implication)	**Principal and Chief Executive**	**Head of Student Entitlement**
	Student disciplinary records	Good Practice		After course ends		
Facilities	Accommodation records / utilization statistics / property strategy	Good Practice	6 years +1			
	Conditions Survey		10 years			

Area of College	Record	Reason (Regulations or Legislative Act)	Period of Retention	Comment	Responsibility (EMT) & formal responsibility for disposal.	Operational Responsibility
	Medical records kept by reason of COSHH regulations		40 years		**Deputy Chief Executive – Business Success** **Deputy Chief Executive – Business Success**	**Estates Manager** **Estates Manager**
Faculties	Student Profile Review (SPR) documents	Good Practice	1 year +1	After course ends	**Assistant Principals**	**Personal Tutor**
	Student references	Good Practice	Narrative reference – 3 years+1 Attendance / achievement record – 6 years +1			
	Student Portfolios	Good Practice	3 months	After course ends		**Course tutor**

Area of College	Record	Reason (Regulations or Legislative Act)	Period of Retention	Comment	Responsibility (EMT) & formal responsibility for disposal.	Operational Responsibility
	Student Coursework	Good Practice	3 months	after course ends		**Course tutor**
Marketing	College Surveys	Good Practice	6 years +1		**Principal and Chief Executive**	**Marketing, PR & Comms Manager**
	Customer Comments	Good Practice	6 years +1			
	Promotional data	Good Practice	2 years +1			
Workforce Development	ESF documentation	Good Practice	6 years +1 after course ends unless ESF related, in which case: For enrolments between calendar years 2007 and 2013, records retained until at least 31/12/2022		**Deputy Principal and Chief Executive**	**Contracts and Employer Responsive Manager**

Area of College	Record	Reason (Regulations or Legislative Act)	Period of Retention	Comment	Responsibility (EMT) & formal responsibility for disposal.	Operational Responsibility
			For enrolments between calendar years 2014 and 2020, records retained until at least 31/12/2030			
	Job Centre records / client files	Good Practice	6 years +1	after contract end date		
	Learn Direct	Good Practice	6 years +1			
Community & Skills for Life & Learning Support	LSC Learning Support form (White form) Learning Support records Additional Support forms	Good Practice	6 years +1	After course ends	**Principal and Chief Executive**	**Learning Support Manager**

	Diagnostic Result Sheet					
Quality	Lesson observation records	Good Practice	3 years +1		**Principal and Chief Executive**	**Quality Managers**
	At least one copy of formal college promotional data to be held as a reference copy		6 years +1			**Head of Communication and Marketing**
Libraries	At least one copy of formal college promotional data to be held as a reference copy	Good Practice	Historical records to be kept permanently		**Principal and Chief Executive**	**Clerk to Corporation**
	Minutes, papers and other records of Corporation meetings and its committees					
Child Protection	Child protection documents / records		25 years after course ends		**Principal and Chief Executive**	**Safeguarding Manager**
College wide	Line Manager's staff files	Good Practice	Duration of individual's employment		**EMT**	**All Line Managers**
	Complaints		6 years +1		**Principal and Chief Executive**	**Principal's Office**
	Routine Correspondence	Good Practice	3 months		**EMT**	**All Staff**

	Non-routine correspondence	Good Practice	1 year +1		**EMT**	**All Staff**
	Bids, funding / grant applications and returns	Good Practice	As per the requirements of the funder		**EMT**	**Relevant Manager proposing bid / tender**