CITY OF WOLVERHAMPTON COLLEGE

Data Retention & Erasure

Policy and Procedure 2023-24

Data Protection Officer

Publication Date: August 2018 | Version No. 1.0
Reviewed August 2023

European Union
European
Social Fund

CITY OF WOLVERHAMPTON COLLEGE
DATA RETENTION & ERASURE POLICY

Revision History

Version	*Revision Date*	*Reviewed / Revised by*	*Section Revised*
1.0	09/05/18	Asst. Mgr. – M. I. S.	New Document
1.0 Reviewed Aug 2020	n/a	Data Protection Officer	n/a
1.0 Reviewed Oct 2021	n/a	Data Protection Officer	n/a

Document Control

Document Owner:	***Document No:***	***Status:***	***Date Approved:***
Data Protection Officer	***1.0***	Approved	***24th May 2018***
Security Classification:	***Next Review Date:***	***Version:***	***Department:***
Low	***August 2024***	V1.0	Funding & Compliance

1 Policy Statement

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.

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.

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

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 Purpose

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.

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 Scope

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 Personal Information and Data Protection

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.

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***, 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.

Our Data Retention Policy and processes comply fully with the GDPR's fifth 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 Objectives

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

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.

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 bodies 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 Guidelines & Procedures

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.

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

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

- **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.

6.1 RETENTION PERIOD PROTOCOLS

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.

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
- Where it is not possible to define a statutory or legal retention period, as per the 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
- Have processes in place to ensure that records pending audit (with particular reference to the requirements of European Social Fund match funding and related retention periods), litigation or investigation are not destroyed or altered
- 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*)

6.2 DESIGNATED OWNERS

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.

6.3 DOCUMENT CLASSIFICATION

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 flows of data within the College.

We also carry out regular Information Audits which enable us to identify, categorise and record all personal information obtained, processed and shared by our college in our capacity as a controller and processor and has been compiled on a central register which includes: -

- What personal data we hold

- Where it came from
- Who we share it with
- Legal basis for processing it
- What format(s) is it in
- Who is responsible for it?
- Retention periods
- Access level (*i.e. full, partial, restricted etc*)

Our information audits and registers enable us to assign classifications to all records and data, thus ensuring that we are aware of the purpose, risks, regulations and requirements for all data types.

We utilise 5 main classification types: -

1. **Public** - information that is freely obtained from / available to the public and as such, is not classified as being personal or confidential
2. **Protect**- information or a system that processes information that belongs to an individual and is classed as personal under the data protection laws
3. **Confidential** – special category and information deemed sensitive (eg medical conditions, disciplinary records etc) that must be secured at the highest level and are afforded access restrictions and high user authentication

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.

6.4 Suspension of Record Disposal for Litigation or Claims

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.

6.5 Storage & Access of Records and Data

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. Documents are always retained in a secure location, with authorised personnel being the only ones to have access. Once the retention period has elapsed, the documents are either reviewed, archived or confidentially destroyed dependant on their purpose, classification and action type.

7 Expiration of Retention Period

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.

7.1 DESTRUCTION AND DISPOSAL OF RECORDS & DATA

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.

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 (GDPR) / current data protection legislation, and that staff are trained and advised accordingly on the procedures and controls in place.

7.1.1 Paper Records

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 Company utilise secure confidential waste collection receptacles and contracted on-site shredding services to dispose of all paper materials.

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.

7.1.2 Electronic & IT Records and Systems

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.

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.

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.

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.

7.1.3 Internal Correspondence and General Memoranda

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.

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

8 Erasure

In specific circumstances, data subjects' have the right to request that their personal data is erased, however the College recognise that this is not an absolute *'right to be forgotten'*. Data subjects only have a right to have personal data erased and to prevent processing if one of the *below conditions applies: -*

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data must be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

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.

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.

Where we receive a request to erase and/or remove personal information from a data subject, the below process is followed: -

1. The request is allocated to the Data Protection Officer and recorded on the Erasure Request Register
2. The DPO locates all personal information relating to the data subject and reviews it to see if it is still being processed and is still necessary for the legal basis and purpose it was originally intended
3. The request is reviewed to ensure it complies with one or more of the grounds for erasure: -

a. the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed
b. the data subject has withdrawn consent on which the processing is based and where there is no other legal ground for the processing
c. the data subject objects to the processing and there are no overriding legitimate grounds for the processing
d. the personal data has been unlawfully processed
e. the personal data must be erased for compliance with a legal obligation
f. the personal data has been collected in relation to the offer of information society services to a child

4. If the erasure request complies with one of the above grounds, it is erased within 30 days of the request being received
5. The DPO writes to the data subject and notifies them in writing that the right to erasure has been granted and provides details of the information erased and the date of erasure
6. Where the College has made any of the personal data public and erasure is granted, we will take every reasonable step and measure to remove public references, links and copies of data and to contact related controllers and/or processors and inform them of the data subjects request to erase such personal data

If for any reason, we are unable to act in response to a request for erasure, we always provide a written explanation to the individual and inform them of their right to complain to 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

8.1 SPECIAL CATEGORY DATA

In accordance with GDPR requirements and current UK data protection 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.

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.

9 Compliance and Monitoring

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.

10 Responsibilities

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.

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.

11 Retention Periods

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)*

12 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 Chief Executive – Business Success**	**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 Chief Executive –**	

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			**Business Success**	**Estates Manager**
HR	Personnel files (including notes of formal hearings)	1980 c58 Limitation Act	6 years +1	From end of employment	**Deputy Principal – Student Engagement**	**HR Manager**
HR & Payroll	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**
	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
				after this ceases	**Deputy Principal – Student Engagement**	**HR Manager**
HR & Payroll	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		
	Sickness/health records	Good Practice	6 years +1	after termination of employment. 40-60 years if H&S/Equality Act potential claims		**Payroll Manager**
Payroll						**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 Chief Executive – Business Success**	**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 – Student Engagement**	**Safety, Health, Fire and Environment 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 Chief Executive – Business Success**	**MIS 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 Chief Executive – Business Success**	**MIS Manager**
	Timetables	Good Practice	1 year +1			
IT Services	Software licenses and hardware registers	Good Practice	5 years +1	After expiry of license	**Deputy Chief Executive – Business Success**	**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 implications)	**Deputy Principal – Student Engagement**	**Head of Student Entitlement**
	Student disciplinary records	Good Practice		After course ends		
Facilities	Accommodation records / utilization statistics / property strategy	Good Practice	6 years +1			

Area of College	Record	Reason (Regulations or Legislative Act)	Period of Retention	Comment	Responsibility (EMT) & formal responsibility for disposal.	Operational Responsibility
	Conditions Survey		10 years		**Deputy Chief Executive – Business Success**	**Estates Manager**
	Medical records kept by reason of COSHH regulations		40 years		**Deputy Chief Executive – Business Success**	**Estates Manager**
Faculties	Student Profile Review (SPR) documents	Good Practice	1 year +1	After course ends	**Vice Principal – Student Success**	**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		**Deputy Principal – Student Engagement**	**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 +1after 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 Chief Executive – Business Success**	**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)	Good Practice	6 years +1	After course ends	**Deputy Principal – Student Engagement**	**Learning Support Manager**
	Learning Support records					
	Additional Support forms					
	Diagnostic Result Sheet					

Quality	Lesson observation records	Good Practice	3 years +1		**Deputy Principal – Student Engagement**	**Quality Manager**
	At least one copy of formal college promotional data to be held as a reference copy		6 years +1			**Marketing, PR & Comms Manager**
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		**Deputy Principal – Student Engagement**	**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**	**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**	**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**