Policy Title **RECORDS MANAGEMENT (INFORMATION STRATEGY FRAMEWORK)**

Author/Responsible Manager	Director of Governance and Compliance
Original Issue Date	September 2013
Approved By and Date	July 2025
Next Review Date	July 2026
EIA Completion date	June 2025
Risk Assessment (please note here any identified risks of non-compliance with the policy)	**Contravention of legislation** Environmental Information Regulations 2005 Data Protection and General Data Protection Regulation 2018 FOI Act 2000

CONTENTS   PAGE NUMBER

Equality Impact Assessment				
Characteristic	**No impact**	**Positive impact**	**Negative impact**	**Evidence**
Race	☐	☒	☐	
Disability	☐	☒	☐	
Gender	☐	☒	☐	
Pregnancy/Maternity	☐	☒	☐	
Religion/belief	☐	☒	☐	
Sexual orientation	☐	☒	☐	
Age	☐	☒	☐	
Gender reassignment	☐	☒	☐	
Marriage & civil partnership	☒	☐	☐	
Carried out by: T Breeze				

Actions required:

Action	Date	Reviewed by	Date

1.   Introduction

A College records management policy is vital to the efficient running of daily operations and underpins the College's legal and regulatory compliance:

- Freedom of Information Act 2000

- Environmental Information Regulations 2004

- Data Protection and General Data Protection Regulation 2018

There is an explicit link between records management and legislation.

Information captured as a record on paper or electronically, including within an email, requires consistent, systematic and active management from the time it is created until it is disposed of either by a controlled destructive process or to an historical archive.

This policy applies to security of information in respect of Kendal College but also for all elements of information security linked to associated delivery (e.g. as part of a consortium or sub-contracting arrangement) and identifies the responsibilities of all staff to ensure that data remains secure and is held in line with legislative requirements. This policy should be read in conjunction with the College's Data Protection Policy and Cyber Security Policy.

2.   Policy Statement

The College holds a record/information lifecycle to identify the series of phases for creation to disposal with the lifespan, usually predetermined. Good records management is based on the principle of regular review and controlled retention and destruction.

The aim is that each record must be managed and maintained in such a way that it:

- Meets internal business needs

- Defends the College and its people against external demands e.g., Freedom of Information requests/ Subject access requests

- Is compliant with regulatory and statutory requirements

- Is capable of providing the primary and secondary evidence of a transaction of business process which is admissible in a court of law

- Is kept and maintained in the most economical way

- Is disposed on in a way that is auditable

The policy covers the following key areas:

a)   Records Creation

b)   Filing Classification Scheme

c)   Retention Schedule

d)   Storage and Maintenance of Records

e)   Final Disposition of Records – historical archive or destruction

f)   Code of Practice & Legislation

g)   Safe handling of data and reduction of risk

Definitions

Data – paper, audio, video, metadata or electronic information that is biographical about living people

Record – outputs that record each and every business or administrative transaction that must remain unaltered across time. The signed version is the "original" in law and includes details about students, staff and external contracts. A record is either paper based or electronic. They form the "collective memory" of the College and must be available beyond the memory or working life of a staff member

Document – a document is work in progress by an individual or group. In its final form it becomes a record. Formal document management systems are widely used to control and track development through versions and editing. The final version will become a record.

Permanent Records – required for the length of existence of the College to comply with legal requests and form part of the historical archive of the college since incorporation in 1993. Permanent records include minutes of the Corporation and audited annual accounts.

Time-limited – records used on a regular basis then maintained for legal reasons in line with retention periods. Time limited information has two phases, firstly it is current information that may be used on a daily or weekly basis. Phase 2 is when it has to be maintained for legal or other reasons but is no longer required for operational purposes. At this point the retention period is applied. Eg student records – used while the student is current but then maintained for several years afterwards and may be required on an occasional basis.

All data and information generated by the College or any of its linked activities including subcontracting, satellite businesses including Kendal Museum are in scope for this policy.

Retention Periods

Retention periods for data are determined by statute, legal, regulatory or business compliance and follow a predetermined request

- Fixed number of years from creation
  Eg financial records kept for current year + 6 years (VAT & Tax)

- Life of transaction + fixed period
  Eg commercial contracts – life of contract + 6 years

Freedom of Information Act 2000

The Act gives every member of the public the right of access to information held by public authorities. The Act requires the College to maintain a publication scheme, agreed through our College registration with the Information Commissioner's Office

(ICO) and to respond to requests under Freedom of Information within a specified timeframe.

Data Protection Act 2018 and GDPR

This Act is concerned with protecting the rights of individuals to their personal data. The law makes a requirement on the College that control or processing of data must be:

- Processed lawfully & fairly
- Obtained only for a specified purpose
- Adequate, relevant and not excessive
- Accurate
- Only kept as long as necessary
- Kept securely

European Social Fund Contracting

The College has previously delivered a number of contracts relating to ESF match provision either through holding a direct contract or as a sub-contractor of a main ESF contractor. The College undertakes to retain records in line with the contractual agreement agree at the outset of delivery and will ensure that the time allocation is noted on the records in line with the procedure below. The current retention period is 25 years from project completion.

3. Procedure

3.1 Records Creation

Records are created for many reasons across the College. Staff are required to use established systems whenever possible using software such as the Prosolution suite for student records and analysis.

3.2. Retention Periods for Records

Records must be retained in line with published requirements. Periods of time, from months to permanency, during which a record has to be maintained by the College, usually determined by legal or regulatory compliance.

A full listing of educational documents and their retention requirements is available from JISC on https://www.jisc.ac.uk/guides/records-retention-management

A summary of key college documents is available at Appendix B. Responsibility for ensuring compliance lies with the relevant head of service. The period is the same for paper or electronic records.

3.3. Storage Options for Paper Records

The College paper archives held securely in a designated area of the college and can only be accessed with the permission of a College Senior Manager or Estates Manager. All archive boxes must be stored on the appropriate rack in the archive area and not left on the floor. The archive area must not be used for general storage of unwanted files or other materials that are not **required** to be stored in line with the retention schedule.

At the end of each academic year, paper documents that require archive storage must be placed in an archive box available from the estates team and clearly labelled with the date of storage and the date for disposal. It is the responsibility of the relevant service manager to ensure retention periods are accurately adhered to.

Student files that are not required to be retained for assessment or longer term purposes must not be archived but will be stored for distribution in line with the Student File policy, clearly indicating the required learner document retention period from the relevant awarding body.

Plastic wallets and hard backed files must not be used for archive materials as they cannot be shredded at point of disposal.

3.4. Destruction Options for Records

Section heads are responsible for ensuring that their archive section is well managed and that clear instructions on destruction are given to the Estates Team who will not be held responsible for errors in destruction.

In June of each year, the Estates Manager will sanction the destruction of archive boxes that have reached their "destroy by" date. All destruction will be carried out by a reputable destruction company to safely and securely destroy any records that have reached their destroy-by date.

3.5. Archived Records – Selection & Management

The archive area is planned to meet the business classification of the records held there. Sections and shelving are labelled as follows:

- Finance
- Human Resources
- Student Records
- Exams
- Student Services
- Governance
- Principal
- European Social Fund (match funding) (Historic records)
- Curriculum Areas (short term storage only)

3.6 Archiving of Electronic Records

This policy should be read in conjunction with any policies on IT usage including that which affects the use of portable and mobile devices which specifies the security requirements to ensure the college complies with Data Protection legislation. Encryption is the minimum standard of adequate security expected by the ICO. Caution must be considered when personal data is being accessed externally that the legislative requirements are being met and where data is being used outside the security of the College network.

The definition of mobile devices includes memory sticks, mobile phones, tablet technologies, netbooks and laptops. Areas of use include the following:

- Learning activities on field trips, work placements and residential visits

- Information provision such as assessment, results, pastoral appointments
- Information gathering eg face to face interview records
- Staff copying central service files to work on at home or note taking in an external meeting

All the above activities may lead to inadvertent or deliberate processing of personal information often for reasons of convenience or ease of use but they do raise issues of consent and confidentiality. Examples of inadvertent breach include sharing of national insurance or passport details of students via email.

Appropriate technical and organisational measures are in place to prevent the unlawful processing of personal data and against accidental loss or destruction of personal data.

Checks on cloud-based or externally managed systems that are not housed on the College servers must be conducted to ensure there is no risk of security breach and the IT Network team provided with evidence of security arrangement of any such system already in place or being considered for purchase through licencing (eg Smart Assessor, College IP)

Personal cloud services (e.g. Dropbox, Google Drive) must not be used to store or transmit College records.
- A Data Protection Impact Assessment (DPIA) must be completed where new systems/processes involve high-risk personal data processing.
- Staff accessing data off-site must use College-approved devices with encryption and VPN security.

3.7 Individual Responsibility for Managing Records

All College staff who create, receive, and use records have records management responsibilities. Individual employees must ensure that the business functions and activities for which they are responsible are documented and recorded appropriately. They must also ensure that the records they create and for which they are responsible are:

- fit for purpose;
- accurate;
- appropriately secure;
- accessible in both the intellectual and physical sense to those with a right to see them; and
- maintained and disposed of in accordance with the College's records management guidance

Mandatory annual training on data protection and records handling is required.

3.8 Retention of Email

Users should ensure that email messages that they intend to keep are properly and orderly filed away so that they can be accessed and retrieved with the same level of content integrity, authenticity, and confidentiality.

There are three classes of information that are processed using the email system and each must be managed in accordance with this policy and the Data Protection legislation. Email use must be consistent with high standards of business conduct and will be determined by their "lasting value" as determined by the relevant head of school or function.

In line with JISC guidance, email accounts of staff members who leave the organisation will be deleted after 6 months.
Refer to End of Employment checklist for line managers to complete prior to the final day of employment.
The classes and their disposal arrangements are:

Personal/Private – dispose of as soon as read. They do not reflect the business of the college and often relate to personal/family arrangements, unsolicited information, social, etc

Ephemeral – dispose of as part of daily administrative routines. These emails facilitate business activities and include copies of minutes, notices of meetings, internal notices to staff.

Corporate – retain in line with the record retention schedule. These emails form part of College records and include business correspondence from external organisations, records of formal approvals, records of actions taken.

The College will agree a default retention period for all non-archived emails and responsibility for adherence to this period will lie with the individual user and not the IT network team. Centralised archiving of key corporate emails is required.

Any emails older than one year old will be automatically moved from the staff members inbox to the online archive. Emails can then be deleted centrally after a set time in line with the retention schedule.

4.   **Documentation**

Appendix A   Key College Documents Retention Schedule

5.   **Links to other policies**

Storage of Student Files
Data Management
Freedom of Information
Information Sharing

Key College Documents Retention Schedule

The length of time documents and records need to be retained by the College is complex and the following information should be used as a minimum guideline. Very specific information on the retention period required for all aspects of data held by the college is available on the following web-link to Jisc Legal:

https://www.jisc.ac.uk/guides/records-retention-management

The guidelines apply to both electronic and hard copies

Area of Work	Examples of Document type	Retention Period
Governance	• Legal framework • Minutes of Corporation & Committee meetings • Register of interests • Appointment of Governors • Strategic planning & operating plan • Risk management • Audits and responses • Complaints • Legal advice • Contracts with 3rd parties • Complaints procedures • Public complaints	− Life of the college − Current + 50 years − Termination of appointment + 6 years − Termination of appointment + 6 years − Superseded + 10 years − Current + 10 years − Current + 5 years − Current + 5 years − Life of the college − Termination + 12 years − 5 years − 3 years
Marketing & IAG	• Course information • Prospectus • Record of course fees • Marketing policy • Press releases	− Superseded + 2 years − Master copy – permanently − Length of course + 6 years − Superseded + 5 years − Issue + 5 years
Curriculum & Quality	• Teaching & Learning policies • Observation records • External quality reviews • Timetabling • Registers • Qualifications lists • Course materials • Student work • Assessment Records • Records of malpractice or suspected malpractice (In an investigation involving a criminal prosecution or civil claim) • Records of the appeal of assessment decisions	− Superseded + 10 years − Current + 5 years − Next review + 5 years − Current + 1 year − Current 1 year − Completion + 10 years − Length of course − Current until EV check/certification plus 12 weeks − Completion+ 10 years − 3 Years − 6 Years − 6 Years
Student Support	• Records of funds eg LSF • Initial assessment, quals on entry • Student complaints – procedures • Student complaints – records	− Current + 6 years − End of college + 6 years − Permanent − Last action + 6 years

Area of Work	Examples of Document type	Retention Period
	• Student associations/union/activities • Student disciplinary records • Careers advice • Learning support records • Student support records • Counselling records	– Permanent – Last action + 6 years – Enrolment + 3 years – Current + 7 years – Current + 6 years – Current + 2 years
Human Resources	• Advertising of new posts • Record of unsuccessful applicants • Record of successful candidates • Induction and training • Performance assessment • Contract of employment • Job description • Pay reviews	– Completion + 6 months – Completion + 1 year – Termination of employment + 6 years – Current + 5 years – Current + 3 years – Termination + 6 years – Duration of job + 1 year – Current + 5 years
Student Data	• Core student data for references • Analysis of student data • Withdrawal records • Exam timetabling • Student enquiries • Analysis of recruitment, retention • Successful applications • Unsuccessful applications • Enrolment data • Personal data on students • Analysis of student data • Academic progress	– Completion + 10 years – Current + 5 years – Termination + 6 years – Current + 1 year – Current + 1 year – Current + 5 years – Completion of course + 6 – Current year + 1 year – End of college + 6 years – Termination of relationship + 6 years – Current academic year + 5 years – Termination of relationship + 6 years
Finance & Funding	• Audit reports • Finance policies • Operational finance eg annual accounts, tax returns, orders • Annual funding allocations • ESF project funding allocations • Payroll • Payment of employer contributions • Payment of employee contributions • Tenders • Insurance – employer's liability • Insurance – all other	– Current financial year + 10 years – Superseded + 10 years – Current financial year + 6 years – Current + 10 years – Current + 6 years (but all other ESF 25 years) – Current + 6 years – Termination of contract + 75 years – Termination + 75 years – Termination + 6 years – Renewal of policy + 40 years – Expiry of policy + 6 years
Miscellaneous	• Record of notification of data controller details to the Office of the Information Commissioner • Requests for personal information • College publication scheme • Trade union records documenting agreements • Trade Union consultations and meeting minutes	– Expiry + 6 years – Last action + 6 years – Completion + 5 years – Completion + 10 years – Completion + 20 years -
ESF	• Contractual agreements • Learner records	– Completion + 25 years (or data identified within the contract)