ETC International College

Documentation Retention and Secure Storage Policy

January 2024

Contents:

1.0 Scope and Purpose

1.1 The purpose of this policy is to outline ETC International College's arrangements for documentation retention and secure storage.

1.2 This policy is for all staff to follow and implement.

1.3 This policy covers all documentation, both paper and electronic, that are either created or maintained by ETC International College (ETC), establishing time schedules of retention for types of documents.

1.4 It is important to implement a document retention policy so ETC can retain only necessary information for the required period of time. This policy will outline what information should be kept, how it should be stored or archived and when it should be deleted in line with GDPR (General Data Protection Regulations) and the Freedom of Information Act 2000. This will enable time and space efficiency throughout the organisation.

1.5 It is important to have efficient and effective processes for document retention and storage to:

- Easily retrieve information when required
- Keep information safe from damage, theft or loss
- Prevent or correct inaccuracies or changes in information
- Protect personal information
- Comply with legal and regulatory requirements
- Minimise storage requirements by only keeping what is necessary.

2.0 Responsibility

2.1 All staff are responsible for efficient data management within their department.

3.0 Retaining Information

3.1 GDPR's Article 5 specifies that personal data should 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')."

3.2 ETC limits the processing and storage of information to only what is required for the purpose of the functioning of the business, the delivery of goods or services and evidence of customers, representatives, transactions, employment and other activities.

3.3 Any inaccurate information should be updated as soon as possible and any irrelevant or inaccurate data should be deleted.

3.4 The information should only be kept for the length of time that it is required for processing the data and the data should be kept securely with measures in place to keep it from being stolen, damaged or lost.

3.5 Organisations must have consent from the individual to process their data, provide individuals access to the data they have and erase all data from systems if this is requested by the individual.

4.0 Preventing Damage, Theft or Loss

4.1 Records must be kept safe from damage, including environmental damage. Archive rooms should be well ventilated, dry, with no direct sunlight and checked regularly for damp or damage to the room.

4.2 Security is vital in keeping all document types safe. Keys should be kept secure and distributed to only those with permission to access the files.

4.3 Files stored on a computer can be at risk of being lost or damaged if the computer gets a virus or the hardware fails so computers and systems should be maintained regularly, with robust anti-virus software installed and regular back-ups programmed.

4.4 Data stored using cloud based facilities are prone to attacks from hackers. Strong passwords should be used and changed frequently.

4.5 Consider what information needs or should be shared on a cloud based facility and issues access only to necessary individuals with permission.

4.6 It is advised to use digital encryption for any personal or sensitive information stored using cloud based facilities.

4.7 When filing is not kept up-to-date it can be hard to find the required information. Information that is incorrectly stored or not yet filed can be time consuming to find. Staff should ensure filing is done in a timely manner to ensure quick and efficient retrieval when needed. Everyone in the company should follow the same process and indexing system for filing so files can be easily searched (where possible) and retrieved and will ensure the correct versions of documents are being used.

5.0 Archiving information

5.1 Deciding when to archive information depends on space available and required retention periods.

5.2 Where there is limited space, information that is legally required to be retained should take priority.

5.3 Information which is no longer actively needed, but must be kept can be archived. This means it can be kept in another secure location to free space up for new and current information. Physical information can be placed in labelled boxes and transported to another secure room, building or storage facility. The boxes should clearly state what is in the boxes with a unique number, list of contents, date of archive, retention period and the date to be destroyed. This information should be linked to a digital labelling system for easy retrieval.

5.4 Alerts can be scheduled as notifications as to when data should be destroyed.

6.0 Retrieval of Information

6.1 Organisations should have procedures in place for retrieving information so that only those with permission can access the information. The retrieval of information should be limited to those that have permission to access it, so a password, key or code should be used for access.

6.2 To retrieve archived information, some staff may need to ask permission from the person in charge of the archived documents and explain what they wish to access and for what reasons. Once permission is granted the person in charge of archive will be able to use the archive database and indexing system to retrieve the information, whether it be physical or digital.

6.3 Retrieval of information should be restricted to only those with permission to access and a log should be kept to track access.

6.4 Some information may not be permitted to leave the archive room.

6.5 Digital information that should not be altered should be shared (only when necessary) as 'read only'.

7.0 Destruction of Data

7.1 Businesses should also follow the Freedom of Information Act 2000, which explains that data that is no longer needed must be destroyed securely.

7.2 There should be no risk that the data could be re-constructed or re-used.

7.3 Any backups or copies of destroyed data should also be destroyed fully, regardless of their data type.

7.4 All filing and records should be up-to-date to ensure the destruction of the correct information at the correct time.

8.0 Associated Documents

8.1 Data Protection and Privacy Policy

9.0 Document Retention Schedule

9.1 The School will seek to balance the benefits of keeping detailed and complete records (for the purposes of good practice, archives or general reference) with practical considerations of storage, space and accessibility. The following legal considerations apply to independent schools in respect of retention of records and documents which must be borne in mind. These include:

- statutory duties and government guidance relating to schools, including for safeguarding
- disclosure requirements for potential future litigation
- contractual obligations
- the law of confidentiality and privacy
- GDPR and UK domestic Data Protection Act 2018 (DPA).

Type of Document	**Retention Period**	**Notes**	**Action after period**	**Action complies with…**
Certificate of Incorporation	Permanently		Archive	
Memorandum and Articles of Association	Permanently		Archive	
Agendas and Minute of Meetings for Board of Governors	Permanently		Archive	
Minutes of Senior Management Meetings	7 years after end of academic year		Destroy	
Minutes of Team Meetings	7 years after end of academic year		Destroy	
Annual Reports	Permanently		Archive	
Policy Documents	6 years after being inactive		Destroy	
Employee Records				
Current Staff Details	Retain			
Job applications , interview records and CVs of	1 year	The applicant must express written	Destroy	

unsuccessful candidates		agreement for their information to be kept on file		
Job applications , interview records and CVs of successful candidates	Retain		Transfer to personnel file	
Personnel Records (including training, disciplinary and work time records)	7 years after termination of employment	For current staff: check for updated information annually, or when necessary	Destroy	
Payroll and wage records (also overtime, bonuses, expenses)	7 years		Destroy	HMRC
Income tax records (P45, P60, P58, P48, etc.)	7 years		Destroy	Taxes Management Act 1970
Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence	3 years after the end of the tax year in which the maternity period ends		Destroy	
Redundancy Records (calculations, payments, refunds, notification to the Secretary of State)	7 years from the date of redundancy		Destroy	
Statutory Sick Pay records, calculations, certificates, self-certificates	7 years after termination of employment		Destroy	

Pension documents	7 years after termination of employment		Destroy	
Exit Interview Forms	7 year after interview		Destroy	
Health and Safety				
Risk Assessments	3 years after the date of assessment		Destroy	
Accident report book	3 years from date of last entry	If the accident involves a child / young adult then until that person reaches 21.		
Public Liability Policies	Permanently			
COSHH Health and Safety Records	40 years			
Fire Safety Certificates	Permanent		Archive	
Fire Incident Records	6 years after date of occurrence		Destroy	
Accounting and Financial Records				
Bank Records	7 years			
Income tax and NI returns, income tax records and correspondence with HMRC	7 years after the end of the financial year to which they relate			HMRC
Records of student fees	7 years		Destroy	
Invoices	7 years		Destroy	
BACS payments	3 years		Destroy	

Purchase Records	5 years		Destroy	
External Audit of Accounts	Permanently		Archive	
Academic				
Registers	7 years		Destroy	
Student Records	7 years		Destroy	
Placement and Proficiency Tests	7 years		Destroy	
Assessment Materials	1 year after the end of the academic year		Destroy	Legislation
Teaching Materials	Continuously Updated			
Examination papers	End of the academic year		Archive	
Approval of Awarding Bodies	Destroy at expiration		Destroy	
External Quality Audit Reports	Permanent		Archive	
Exam Results	10 years		Destroy	
Assessment Board Meeting Minutes	10 years		Destroy	
Assessment and internal verification records (including RPL records)	3 years after certification			
Marketing				
Promotional Material	Permanent		Archive	
Brochures / Prospectuses / Dates and Fees	Permanent		Archive	

ETO (Educational Tour Operator) details	7 years after inactivity		Destroy	
ICT				
CCTV recordings	28 days	Unless needed for legal requirements	Destroy	
Emails	1 year		Archive	

Version: 2
Approved January 2024: Board of Governors
Next update due: January 2027