SECAT

RECORDS MANAGEMENT POLICY

Status: .... Statutory

Updated: .... December 2025

Reviewed and ratified by: .... SECAT Leadership Team

Signed by Trust/Committee Chair

Next review date: …………………….. December 2026

Published location: .... www.secat.co.uk

Version History

V24.1	October 2024	Updated policy template in accordance with latest advice from the Information Commissioners Office and BS10025-2021: “Management of records – Code of practice” outlining what should be included within a Records Management policy. New sections include: • Our approach and commitment to records management • Related policies and processes • Roles and responsibilities • What constitutes a record • Storage of Records: Emails • Monitoring compliance

Whilst SBM Services (uk) Ltd will endeavour to ensure that all tools and resources are reflective of current legislation and guidance, the Client is solely responsible for the appropriate use and adaption of The SBM Toolkit tools and resources for their own use. The Client is also responsible for seeking appropriate financial, legal and technical advice; using resources within The SBM Toolkit does not take the place of appropriate technical advice.

Records Management Policy

This policy provides the framework the trust will follow to achieve effective management and audit of records.

The role of records management

SECAT recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations and to contribute to the effective overall management of the institution. Records provide evidence for protecting the legal rights and interests of the trust and provide evidence for demonstrating performance and accountability.

Our approach and commitment to records management

SECAT undertakes to manage records in relation to the three principles of value, integrity and accountability laid out in the Lord Chancellor's Code of Practice issued under Section 46 of the Freedom of Information Act 2000, published in July 2021.

Related policies and documents

- Retention Schedule
- Data Protection policy
- Freedom of Information policy
- Data breach process
- Third party request for data process
- Other related legislation and regulations such as equal opportunities and ethics which apply to the school/trust

Roles and responsibilities

The Trust Board will:

- Establish and maintain a positive records management culture.
- Ensure the Trust Data Protection Lead prepares a Records Management policy for approval and adoption by the Trust Board and to review and monitor the effectiveness of the policy.
- Allocate sufficient resources for records management, e.g. in respect of training for staff.
- Monitor and review records management issues.
- Ensure that the Trust provides adequate training, information, instruction, induction and supervision to enable everyone to comply with their responsibilities.

The CEO will:

- Promote a positive records management culture.
- Ensure that all staff co-operate with the policy.
- Ensure that staff are competent to undertake the tasks required of them and have been provided with appropriate training.
- Provide staff with equipment and resources to enable them to undertake the tasks required of them.
- Ensure that those who have delegated responsibilities are competent, their responsibilities are clearly defined, and they have received appropriate training.

The Data Protection Lead

- Provide guidance to staff on good records management practice
- Promote compliance with this policy so that information can be retrieved easily, appropriately and in a timely way
- Check that records are stored securely and can be accessed appropriately at least annually

Staff at the Trust will:

- Familiarise themselves and comply with the Records Management policy
- Properly document their actions and decisions
- Hold personal information securely
- Only share personal information appropriately and will not disclose it to any unauthorised third party
- Dispose of records securely in accordance with the school's/trust's Retention Schedule

What constitutes a record?

A record is any document created, received or maintained by permanent and temporary staff of the Trust / Schools the course of carrying out its functions. Also, by any agents, contractors, consultants or third parties acting on behalf of the Trust / schools

Records are defined as all those documents which facilitate the business carried out by the trust/schools and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronic format.

Storage of records: digital data

Back Up System: The trust will undertake regular back-ups of all information held electronically to enable restoration of the data in the event of an environmental or data corruption incident. Backups are run daily.

The trust tests that data can be restored from a back-up on a regular basis.

Controlling the Storage of Digital Data: Personal information is not to be stored on the hard drive of any laptop or PC unless the device is running encryption software

The Bring Your Own Device policy outlines how data can be accessed and stored on personal devices.

Password Control: The trust will ensure that data is subject to a robust password protection regime and multifactor authentication. Password sharing is forbidden. Staff are required to lock their devices when they are away from them to prevent unauthorised use.

Location of Server Equipment: The school/trust will ensure that the server environment is managed to prevent access by unauthorised people.

Storage of records: emails

Email accounts are not designed to be a records storage system, and therefore emails should not be retained indefinitely. Where an email contains a message or attachment which relates to a pupil, member of staff or contains information that needs to be retained for future reference, the trust requires that this is moved from the individual's email account to the relevant area within the official hard copy or digital data storage system. This content will then fall within the relevant section of the trust's Retention Schedule.

Where emails do not contain information that needs to be retained, they should be deleted at the earliest opportunity and by no later than 30 days and in line with the process outlined within the 'Disposal of Records' section of this policy.

Storage of records: hard copy data

Storage of Physical Records: The trust requires that all physical records are stored in filing cabinets, drawers or cupboards. Sensitive physical records should be kept in a lockable storage area. This is to prevent unauthorised access but also to protect against the risk of fire and flooding.

Unauthorised Access, Theft or Loss: Staff are encouraged not to take personal data on staff or students out of the trust unless there is no alternative.

Clear Desk Policy: In order to avoid unauthorised access to physical records which contain sensitive or personal information and to protect physical records from fire and/or flood damage, the trust operates a clear desk policy. This involves the removal of the physical records to a cupboard or drawer (lockable where appropriate). It does not mean that the desk has to be cleared of all contents.

Retention of records

The trust has documented how long it will retain specific records within its Retention Schedule. This schedule contains recommended retention periods for the different records created and maintained by educational settings in the course of their business. The schedule refers to all information regardless of the media in which it is stored.

Some of the retention periods are governed by statute. Others are guidelines following best practice. Every effort has been made to ensure that these retention periods are compliant with the requirements of data protection legislation.

Managing records using these retention guidelines will be deemed to be 'normal processing' under data protection legislation. If records are to be kept for longer or shorter periods than laid out in the schedule then the reasons for this need to be documented.

Disposal of records

Records should not be kept for any longer than is necessary in relation to the purpose for which they were originally collected/processed. The Retention Schedule sets out the retention periods for all records held by the trust.

All records containing personal information or sensitive policy information should be made either unreadable or unreconstructable.

- Physical records should be place in the confidential waste bins.
- Electronic records should be permanently deleted.
- Emails should be permanently deleted.
- Hardware containing personal information will be collected by an external secure waste company.

If an external company is used for any part of the disposal process, the company must provide a Certificate of Destruction to evidence secure disposal of the record.

Monitoring compliance

The schools Data Protection Leads will check that records are stored securely, in line with the retention schedule and that they can be accessed appropriately at least annually and provide a report for the Deputy Chief Operating Officer.

Other

In the event of an incident involving the loss of information or records held by the trust, the Data Breach process should be followed.

If the trust receives a request for information from a third party, then the process outlined in the Third Party Requests for Information process should be followed.