Records Management Policy

Adopted by SEEAT Board : Autumn 2022
Amendment approved by SEEAT Board: Autumn 2026
Next Review Date: Autumn 2029

To be read in conjunction with the Data Protection Policy and Document Retention and Disposal Guidelines

South East Essex Academy Trust (SEEAT) 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. This document provides the policy framework through which this effective management can be achieved and audited.

1. Scope of the policy

1.1 This policy applies to all records created, received or maintained by staff of the Trust in the course of carrying out its functions.

1.2 Records are defined as all those documents which facilitate the business carried out by the Trust and which are thereafter retained (for a certain period) to provide evidence of its transactions or activities. These records may be created or received, and then stored, in hard copy or electronically.

1.3 A small percentage of the Trust's records may be selected for permanent preservation as part of the institution's archives and for historical research.

2. Responsibilities

2.1 The Trust has corporate responsibility for maintaining its records and record-keeping systems in accordance with the regulatory environment. The SEEAT Board retains overall accountability for records management across the Trust. Headteachers are responsible for implementing this policy within their schools, supported by the Trust's Data Protection Officer (DPO) as appropriate.

2.2 The person responsible for records management in each school will give guidance about good records management practice and promote compliance with this policy so that information can be retrieved easily, appropriately and in a timely way. They will monitor compliance at least annually, including whether records are stored securely, can be accessed appropriately, and are retained and disposed of in accordance with the Trust's approved retention schedule. Data protection or information-governance issues requiring specialist advice should be referred to the Trust's DPO.

2.3 Individual staff and employees must ensure that records for which they are responsible are accurate, and are maintained and disposed of in accordance with the school's records management guidelines.

3. Recording Systems

Information created by the Trust must be managed against the same standards regardless of the media in which it is stored.

Maintenance of Record Keeping Systems

i. Filing and record-keeping must be properly resourced and carried out regularly. Records should be reviewed and disposed of in accordance with the Trust's approved retention schedule. Where a subject access request, Freedom of Information request, complaint, investigation, litigation or other legal hold applies, relevant records must not be altered, destroyed or concealed in order to prevent disclosure and routine destruction must be suspended where necessary until the matter is concluded.

ii. Applying retention periods is straightforward provided files are closed on a regular basis.

iii. Once a file has been closed, it should be moved out of the current filing system and stored either in a record room in each school or in another appropriate place until it has reached the end of the retention period.

iv. Information security is particularly important when handling personal information, special category personal information, confidential information or other sensitive Trust information. Records must be protected by appropriate technical and organisational measures and handled only through Trust-approved systems and processes. The following basic rules apply:

- Paper records containing personal or confidential information must be stored securely, with access restricted to authorised persons;
- Electronic records must be protected by appropriate access controls, including strong authentication and screen locking, in accordance with SEEAT's ICT and information-security requirements;
- Records containing personal or confidential information must not be left unattended where unauthorised persons could access them;
- Personal or confidential information must only be sent electronically using Trust-approved systems and appropriate security measures. Staff must follow Trust guidance on encryption, secure sharing and password protection where applicable;
- Records should only be taken off-site where there is a legitimate business need and this is permitted by SEEAT procedures. They must remain secure and protected against loss, theft, damage and unauthorised access;
- Personal or confidential information must not be stored on removable media unless the media is Trust-approved, its use is necessary and authorised, and appropriate encryption and security controls are applied;
- Electronic information must be stored on Trust-approved systems that are appropriately backed up and recoverable in accordance with SEEAT's ICT arrangements;
- Emails and other communications that constitute an official record must be saved to the appropriate Trust-approved record-keeping system and retained in accordance with the relevant retention category.

4. Managing Pupil Records

The pupil record should be seen as the core record charting an individual pupil's progress through the Education System. The pupil record should accompany the pupil to every school they attend and should contain information that is accurate, objective and easy to access. These guidelines are based on the assumption that the pupil record is a principal record and that all information relating to the pupil will be found in the file (although it may spread across more than one file cover).

5. File covers for pupil records

It is strongly recommended that schools use a consistent file cover for the pupil record.
This assists each school to ensure consistency of practice when receiving records from a number of different schools. By using pre-printed file covers all the necessary information is collated and the record looks tidy and reflects the fact that it is the principal record containing all the information about an individual child.

6. Recording information

A pupil, or a person entitled to act on their behalf, may have rights of access to personal information held about them under the UK GDPR and Data Protection Act 2018, as amended. Requests must be handled in accordance with the Trust's data protection procedures. All information recorded about pupils should be accurate, objective, relevant and expressed in a professional manner.

The pupil record starts when a record is created for each new pupil as they begin school. It follows the pupil through their school career in accordance with applicable transfer and retention requirements. The record may include personal information and, where applicable, special category personal information, including:

- Surname
- Forename
- DOB
- Special Educational Needs Yes/No [This is to enable the files of children with special educational needs to be easily identified for longer retention]

- Emergency contact details
- Gender
- Preferred name
- Language of home (if other than English)
- Names of parents and/or guardians with home address and telephone number (and any additional relevant carers and their relationship to the child)
- Name of the school, and the date of admission and the date of leaving
- Biometric information (where applicable).
- Any other medical involvement e.g. speech and language therapist, paediatrician

7. Responsibility for the pupil record once the pupil leaves a school

Where a pupil leaves and moves to another school, relevant pupil records should be transferred securely to the new school in accordance with applicable requirements and Trust procedures. Records retained by SEEAT must be kept for the periods specified in the Trust's approved Document Retention and Disposal Guidelines. Retention periods must be applied by reference to the type and purpose of the record and any applicable statutory, regulatory, safeguarding, contractual or limitation requirements. Records must not be retained solely on the basis of a general assumption that all pupil records must be kept until age 25.

8. Safe destruction of the pupil record

The pupil record should be disposed of in accordance with the Trust's Document Retention and Disposal guidelines.

8.1 Where an external provider is used for confidential destruction, SEEAT must use an approved provider and ensure appropriate contractual, confidentiality and data-protection arrangements are in place where applicable. Records must be protected through a secure chain of custody and destruction must be evidenced by an appropriate certificate, log or equivalent record.

If a record has been identified for destruction but has not yet been destroyed, and it becomes relevant to a subject access request, Freedom of Information request, complaint, investigation, litigation or other legal hold, destruction must be suspended where required and the record preserved until the matter is concluded.

9. International transfers of pupil information

Where pupil personal information is to be sent or made accessible to a separate organisation outside the UK, staff must consult the Trust's DPO before the transfer takes place. Any restricted transfer must comply with the UK GDPR international-transfer rules and be covered by an applicable UK adequacy regulation, appropriate safeguard or permitted exception. The transfer must also comply with the Trust's wider data-protection, information-security and record-transfer requirements.

10. Storage of pupil records

All pupil records should be kept securely at all times. Paper records, for example, should be kept in lockable storage areas with restricted access, and the contents should be secure within the file. Equally, electronic records should have appropriate security.
Access arrangements for pupil records should ensure that confidentiality is maintained whilst equally enabling information to be shared lawfully and appropriately, and to be accessible for those authorised to see it.

11. Good practice for managing e-mail

These guidelines are intended to assist school staff to manage their e-mail in the most effective way, and must be used in conjunction with your school's policies on the use of ICT.
Information about how your e-mail application works is not included in this document.

11.1 As communicating by e-mail is quick and easy, many people have replaced telephone conversations and memos with e-mail discussions. However, the language in which e-mail is written

is often less formal and more open to misinterpretation than a written memo or a formal letter. Remember that e-mail should be laid out and formulated to your school's standards for written communications.

11.2 Staff must consider information security before sending confidential or personal information by email. Such information must only be sent using Trust-approved systems and appropriate security measures, taking account of the nature and sensitivity of the information and the intended recipient. Staff should verify recipients before sending and should avoid placing unnecessary personal or confidential information in subject lines.

11.3 School emails may fall within the scope of requests made under the Freedom of Information Act 2000 or data protection legislation, depending on their content and the information held. This does not mean that every email will be disclosed: applicable exemptions, exceptions and the rights of third parties must be considered when responding to a request. Staff should therefore write emails professionally and on the basis that relevant records may be reviewed or disclosed where the law requires.

11.4 Emails can remain within systems after an individual user has deleted their copy, and copies may also be held by recipients or within authorised backup and archive systems. Emails that are held and fall within the scope of a valid request may need to be considered for disclosure under the Freedom of Information Act 2000, UK GDPR or Data Protection Act 2018, subject to the applicable legal tests, exemptions and exceptions.

12. Monitoring and Review

This policy will be reviewed and approved in accordance with SEEAT's governance arrangements. The Records Management Policy will be reviewed at least every three years, and earlier where changes in legislation, regulatory guidance, Trust systems or operational requirements make this necessary.