SEEAT

SOUTH EAST ESSEX
ACADEMY TRUST

RECORDS MANAGEMENT POLICY

Version Control

Date	Version	Reason	Owner	Author
May 2018	Final	Initial adoption	Executive Principal and SEEAT Board	Data Protection Officer

To be read in conjunction with the:

DP/GDPR Policy
Document Retention and Disposal Guidelines
Records Management Policy

Records Management Policy

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 a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The person with overall responsibility for this policy is the Head teacher of each school in the Trust.

2.2 The person responsible for records management in each school will give guidance about good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and in a timely way. They will also monitor compliance with this policy by surveying at least annually to check if records are stored securely and can be accessed appropriately.

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. It is important that filing information is properly resourced and is carried out on a regular basis. It is equally important that the files are weeded of extraneous information where appropriate on a regular basis. Removing information from a file once a subject access or a freedom of information request has been made will be a criminal offence (unless it is part of normal processing).

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 very important especially when dealing with personal information or sensitive policy information. There are a number of basic rules:

- All personal information should be kept in lockable filing cabinets which are kept locked when the room is unattended;
- Personal information held on computer systems should be adequately password protected. Information should never be left up on a screen if the computer is unattended;
- Files containing personal or sensitive information should not be left out on desks over night;
- Where possible sensitive personal information should not be sent by e-mail. Where e-mailed in exceptional circumstances such information should be encrypted and/or password protected.
- If files need to be temporarily taken off the premises they should be secured in the boot of a car or in lockable containers;
- Teachers may carry data on memory sticks or other removable data carriers in order to access their files both at home and at school. Any data carried in this way must be encrypted using appropriate encryption software;
- All computer information should be backed up regularly;
- Information contained in email and fax should be filed into the appropriate electronic or manual filing system once it has been dealt with.

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 their nominated representative has the legal right to see their file at any point during their education and even until the record is destroyed. This is their right of subject access under the Data Protection Act 1998/General Data Protection Regulation. It is important to remember that all information should be accurately recorded, objective in nature and expressed in a professional manner.

The pupil record starts its life when a file is opened for each new pupil as they begin school. This is the file which will follow the pupil for the rest of their school career. The information includes personal and sensitive/special categories data as follows:

- 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 the pupil records should be transferred to the new school. The school which the pupil attended until statutory school leaving age (or the school where the pupil completed sixth form studies) is responsible for retaining the pupil record until the pupil reaches the age of 25 years. This retention is set in line with the Limitation Act 1980 which allows that a claim can be made against an organisation by a minor for up to 7 years from their 18th birthday.

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 it is recommended that all records must be shredded on-site in the presence of an employee. The organisation must also be able to prove that the records have been destroyed by the company who should provide some form of Destruction Certificate/log.

It is important to understand that if the records are recorded as to be destroyed but have not yet been destroyed and a request for the records has been received they MUST still be provided.

9. Transfer of a pupil record outside the EU area

If you are requested to transfer a pupil file outside the EU area because a pupil has moved into that area, please contact the Local Authority for further advice.

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 You need to think about information security when you send confidential information by e-mail. The consequences of an e-mail containing sensitive information being sent to an unauthorised person could be a fine from the Information Commissioner or it could end up on the front page of a newspaper. Confidential or sensitive information should only be sent by a secure encrypted e-mail system. Never put personal information (such as a pupil's name) in the subject line of an e-mail.

11.3 All school e-mails are disclosable under Freedom of Information and Data Protection legislation. Be aware that anything you write in an email could potentially be made public.

11.4 E-mails can remain in a system for a period of time after you have deleted them. You must remember that although you may have deleted your copy of the e-mail, the recipients may not and therefore there will still be copies in existence. These copies could be disclosable under the Freedom of Information Act 2000 or under the Data Protection Act 1998.

11.5 Here are some steps to consider when sending e-mail:

Do I need to send this e-mail?

Ask yourself whether this transaction needs to be done by e-mail? It may be that it is more appropriate to use the telephone or to check with someone face to face.

Who do I need to send this e-mail to?

Limit recipients to the people who really need to receive the e-mail. Avoid the use of global or group address lists unless it is absolutely necessary. Never send on chain e-mails.

Use a consistent method of defining a subject line

Having a clearly defined subject line helps the recipient to sort the e-mail on receipt. A clear subject line also assists in filing all e-mails relating to individual projects in one place. For example, the subject line might be the name of the policy, or the file reference number.

Ensure that the e-mail is clearly written

- Do not use text language or informal language in school e-mails.
- Always sign off with a name (and contact details).
- Make sure that you use plain English and ensure that you have made it clear how you need the recipient to respond.
- Never write a whole e-mail in capital letters.
- Always spell check an e-mail before you send it. Do not use the urgent flag unless it is absolutely necessary, recipients will not respond to the urgent flag if they perceive that you use it routinely.
- If possible, try to stick to one subject for the content of each e-mail, as it will be easier to categorise it later if you need to keep the e-mail.

Sending attachments

Sending large attachments (e.g. graphics or presentations) to a sizeable circulation list can cause resource problems on your network. Where possible put the attachment in an appropriate area on a shared drive and send the link round to the members of staff who need to access it.

Disclaimers

Adding a disclaimer to an e-mail mitigates risk, such as sending information to the wrong recipient, or helps to clarify the school's position in relation to the information being e-mailed. Typically, they cover the fact that information may be confidential, the intention of being solely used by the intended recipient, and any views or opinions of the sender are not necessarily those of the school.

How long to keep e-mails?

E-mail is primarily a communications tool. E-mails that need to be kept should be identified by content; for example, does it form part of a pupil record? Is it part of a contract? The retention for keeping these e-mails will then correspond with the classes of records according to content in the retention schedule for schools found in the Document Retention and Disposal Guidelines. These e-mails may need to be saved into any appropriate electronic filing system or printed out and placed on paper files.

12. Monitoring and Review

This policy has been reviewed and approved by the SEEAT Board.
The Records Management Policy will need to be reviewed and updated as necessary every 2 years.