Retention of Information and Records Policy

This policy applies to all schools in Embrace Multi Academy Trust

Embrace Multi Academy Trust strives to maintain and improve good provision and outcomes at each of its member schools. Based upon our shared ethos and our values of wisdom, collaboration, respect, integrity, inclusivity and compassion, we aim to support the learning and development of every person within the trust and our policies are written from this perspective.

Version	Approval Level	Document History	Date	Review Period
V1	Board of Trustees	Approved	28.03.2023	2 Yearly

1. Introduction

1.1. Embrace Multi Academy Trust is committed to maintaining the confidentiality, security, and integrity of the information it holds.

1.2. The trust recognises that the efficient management of records throughout their lifecycle is necessary to support its core functions, reduce risks and to comply with legal and regulatory obligations.

1.3. This policy sets out how information will be processed, stored, accessed, monitored, retained, and disposed of, to meet the trust's statutory requirements including access to information legislation, data protection legislation and all other associated legislation that the trust is bound by as an educational provider.

2. Aims

2.1. The aim of this policy is to provide clarity and direction for the consistent management of trust records, including:

- roles and responsibilities for managing records at the trust;
- classification scheme for trust records;
- management and storage of records throughout the record's lifecycle;
- management of the full pupil record;
- retention periods;
- disposal procedures;
- audit and review processes.

3. Scope

3.1. This policy applies to all records created, received, or maintained by the trust, regardless of whether they are in hard copy or electronic format.

3.2. This policy applies to all members of staff within the trust. For the purposes of this policy, the term "staff" means all members of trust staff including permanent, fixed term, and temporary staff, governors, secondees, any third-party representatives, agency workers, volunteers, interns, agents, and sponsors engaged with the trust in the UK or overseas.

3.3. The trust recognises that this is a new policy. Whilst it is being implemented from 1 April 2023, there will be a period of adjustment required where schools and departments work towards the updated retention schedule and review and update records management processes and procedures.

4. Definitions

4.1. **Records** are defined as all documents and materials, regardless of format, which facilitate the functions carried out by the trust and provide evidence of its core activities and decisions made. These records may be created, received, or maintained in hard copy or electronic format, including emails.

4.2. The **Records of Processing Activities** (ROPA) is a requirement of the Data Protection Act 2018 and UK GDPR. It captures all the purposes for which the trust processes personal data; the legal basis for processing personal data; who personal data is shared with; and how it is managed.

4.3. The **Information Asset Register** (IAR) is a register detailing the location of key record types, including paper and electronic records. It ensures the trust and schools is able to account for where records are stored, who is responsible for them and how they are retained.

4.4. The **Retention Schedule** provides the statutory, or otherwise agreed, retention periods for how long record types are held before destruction.

5. Associated Legislation and Guidance

5.1. This policy has due regard to the following legislation including, but not limited to, the following:

- Data Protection Act 2018 and UK GDPR;
- Section 46 Freedom of Information Act – Records Management;
- Limitation Act 1980;
- The Education (Independent School Standards) Regulations 2014.

5.2. The trust has due regard to the Information Records Management Society 'Information Management Toolkit for Academies', widely regarded as a leading source of recommended guidance, from which the trust retention policy has been modelled.

6. Roles and Responsibilities

6.1. Trust Board
Statutory responsibility to maintain trust records and records management systems in accordance with legislation.

6.2. Trust Executive Team
Accountable to the trust board for ensuring there are appropriate provisions in place for managing all record types across the trust.

6.3. Principal / Headteacher
Responsible for ensuring this policy is implemented and that all records are stored securely and in accordance with the retention periods outlined.

6.4. Data Protection Officer (DPO)
Responsible for providing guidance and advice on good records management practice and promoting compliance with this policy.

6.5. Trust Network Manager
Responsible for ensuring the technical security and protection of trust records, including continuity and recovery measures in the event of a security incident or breach.

6.6. Line Managers
Responsible for ensuring that their staff are aware of this policy and comply with its requirements. They ensure that when a member of staff leaves, responsibility for their records is transferred to another person; or deleted if no longer required.

6.7. All Staff
Responsible for managing the records in accordance with trust policies and procedures and disposing of records securely, in accordance with the trust's **records retention schedule**.

7. Classification of Records

7.1. All information that the trust creates, receives and shares has value. The trust's **information classification scheme** is intended to support the correct management of records depending on the classification of the information they contain *(table 1)*.

7.2. All records that are classified as confidential must be kept securely and only accessible by authorised staff.

Classification	Definition	Examples
Public	• Data that if lost, stolen, misused or corrupted would have no negative impact on individuals or the trust. • Available to anyone inside or outside of the trust.	• Marketing materials. • Social media posts. • Published newsletters. • Published trust contact details.
Internal	• Data that if lost, stolen, misused or corrupted could have a minor negative impact on individuals or the trust. • Available to all authenticated staff at the trust.	• Policies / procedures / guidelines. • Meeting agendas. • Staff newsletters. • Information intended for future publication.
Confidential	• Data that if lost, stolen, misused or corrupted would have a negative impact on individuals or the trust, the level of which would need careful investigation and may require external reporting to police, ICO or other. • Data that enables the trust to deliver its key functions and services. • The "principle of least privilege" is to be followed at all times: access to data is restricted to authorised staff on a need to know basis.	• Personal data. • Contract and financial information. Exam papers. • Information that would compromise physical and electronic security, such as buildings, IT services, information assets.

Table 1: Information Classification Scheme

8. Creating Records

8.1. The trust and each school is responsible for ensuring maintains its own up-to-date **information asset register** for the records it creates and manages, which must be made available for annual audit reviews.

8.2. The trust expects that key records are maintained in electronic format in order to:

- ensure the ongoing availability the information in back-up o assist in data sharing where appropriate;
- ensure access to information by authorised users;
- minimize duplication of data, eg information stored in a school's management information system will not also be printed and stored in a paper file.

8.3. Schools must risk assess those records held only in paper format, assessing the risks of loss of access, for example through fire or theft, in particular those records of a confidential nature.

8.4. The practice of keeping local versions of records (whether electronic or in paper format) should be avoided unless there is a defined business purpose. Duplicate records maintained should be included in the **information asset register**.

9. Access to Records

9.1. The trust maintains a principle of least privilege access to ensure systems and records containing confidential information are accessible by authorised staff only.

9.2. Under no circumstances are visitors allowed access to confidential information. Visitors to areas of a school containing confidential information must be supervised at all times.

10. Security

10.1. The trust will store key information in DfE approved enterprise-level cloud storage such as Microsoft Office One Drive, to ensure access in the event of school closures.

10.2. Staff must not use computer / laptop hard drives (c:/drive) or desktop to store personal information.

10.3. All electronic devices, including mobile phones, must be password-protected to protect the information on the device in case of theft.

10.4. All members of staff are provided with their own secure network login and password which must not be divulged to anyone else.

10.5. All staff members should implement a clear desk policy to avoid unauthorised access to physical records containing sensitive or personal information.

10.6. The physical security of the trust's buildings and storage locations is reviewed by the trust's estates and compliance manager, school safeguarding leads and the DPO, to evaluate the risks of vandalism, burglary or theft, and provide guidance on measures to reduce risk accordingly.

10.7. Where it is necessary to maintain paper records, these must be kept in a suitable locked cabinet, drawer, safe, or secure space with restricted access.

10.8. Confidential paper records are not left unattended or in clear view when held in a location with general access.

10.9. Memory sticks are not used to hold personal information.

11. Retention and Disposal

11.1. Trust records should be retained for no longer than is necessary and in accordance with the trust **retention schedule** (appendix A).

11.2. Managing records according to the retention schedule is deemed to be "normal processing". Members of staff should be aware that once a freedom of information request has been received or a subject access request, then records disposal must be stopped.

11.3. If any record series are to be kept for longer or shorter periods than those laid out in the retention schedule, the reasons for this need to be documented in each school's information asset register.

11.4. All records produced through the day-to-day operations of the trust containing personal identifying information must be disposed of securely through shredding.

11.5. Where the retention schedule states 'SECURE DISPOSAL', this must be via the trust's confidential waste disposal service which provides confidential waste consoles in all schools, or via a crosscut shredder.

11.6. The trust network manager will provide support and guidance to schools regarding the secure disposal of computer and electronic records through approved recycling services.

12. Information Audits

12.1. Each trust school will maintain an up-to-date information asset register. The DPO will provide support and guidance to individual schools to ensure this is kept up to date.

12.2. Records containing personal data must be logged in the schools IAR to ensure the school meets its obligations under GDPR to have a current data map.

12.3. The DPO will conduct an information audit on an annual basis against all key data assets held by the school to ensure that this is correctly managed in accordance with this policy.

13. Related Policies, Standards, and Guidelines

13.1. The records management policy should be read in conjunction with the data protection policy.

14. Review

14.1. The trust will be responsible for ensuring that this policy and its associated procedures are reviewed annually.

14.2. Date of next review: see front cover.