Records Management Policy

Introduction and Scope

Atomix Educational Trust recognises records management as a core corporate function that supports the effective management of the Trust. A records management programme ensures that authoritative evidence of our work is created, captured, managed and made accessible within the scope of our information governance policy framework. This allows for improved accountability, transparency, continuity, decision-making, and better compliance with relevant legislation and regulations, as well as protecting the rights and interests of ourselves and our pupils.

A record is defined as information created, received and maintained as evidence and as an asset by the Trust in pursuit of legal obligations or in the transaction of business. Records are retained as evidence for a set period determined by legal, regulatory and functional requirements.

The Records Management policy and retention schedule applies to all records created, received or maintained by the Trust in the course of carrying out its functions, regardless of whether it is in paper or electronic format.

This policy applies to all employees, governors or Trustees, contractors, agents and representatives, volunteers and temporary staff working for, or on behalf of, the Trust. It should be read alongside the other policies within our information governance policy framework, including the Data Protection policy, Information Security policy and Acceptable Use policies.

Roles and Responsibilities

Overall responsibility for ensuring that the Trust meets the statutory requirements of any legislation lies with the Board of Governors or Trustees. The following roles have day to day responsibility for records management compliance and provide the necessary assurance to the Board.

Senior Information Risk Owner (SIRO)

The SIRO is responsible for overseeing the implementation of this policy and ensuring that effective records management practices are in place across the Trust. They are ultimately responsible for the day-to-day operational management of the Trust and will ensure that staff are appropriately trained in relation to records management, supported by the SPOC and IAOs. In our organisation this role lies with the CEO.

Single Point of Contact (SPOC)

The SPOC will support the SIRO in the day-to-day operational management of the Trust, providing guidance on good records management practices and promoting compliance with this policy so that information can be retrieved easily, appropriately and in a timely way. They will help develop and carry out regular reviews of the records management programme, at least annually, to ensure compliance and to check that records are stored

securely and can be accessed appropriately. In our organisation this role lies with the Director of Operations.

Information Asset Owner (IAO)

The IAO is responsible for the security and maintenance of a particular record during its lifecycle. They need to understand how information is created, amended or added to over time, and know who has access to the records and why. They are responsible for the appropriate disposal of information when it is no longer required. A record of IAOs is included in our Information Asset Register.

All staff

All staff, including governors or Trustees, contractors, agents and representatives, volunteers and temporary staff working for, or on behalf of, the Trust are responsible for managing records consistently in accordance with this policy. They must keep complete and accurate records which adequately document their work.

Records Management

We have a robust programme in place for managing our records throughout their lifecycle. This includes using methods such as version control and file plans to ensure that records can be easily searched and accessed in the event of an information request. We also include records and information management as a risk on our corporate risk register.

Information Asset Register (IAR)

In accordance with Article 30 of UK GDPR, we have in place an Information Asset Register (IAR) which maintains a record of our processing activities. The IAR documents exactly what records we hold, where they are stored, who has access to the information and the retention periods in place. This is reviewed, at least annually, to ensure it remains accurate.

Email management

We have a process in place to ensure that emails are also managed in line with this policy and our retention schedule. Emails discussing Trust business or reflecting significant actions or decisions concerning Trust business will not be stored in personal email inboxes but will be removed and stored securely in the appropriate filing system.

Personal email inboxes are regularly reviewed by staff to ensure any unnecessary emails are deleted.

Pupil Records

The Trust are under a duty to maintain a record for each pupil which serves as the core record of an individual's progress through the education system and should accompany them throughout their school career. The information within the pupil record must be easy to find, accurately and objectively recorded, and expressed in a professional manner.

Pupil records are held electronically within our management information system (MIS). Some information, not forming part of the core record, will be held outside the MIS in either electronic or paper format. This includes information which has shorter retention periods such as attendance registers, consent forms, medical forms, accident forms, absence notes and pupil work.

Safeguarding files

Records relating to pupils involved with child protection or safeguarding are held securely in a designated system accessible to the Designated Safeguarding Leads (DSLs). This is stored separately to the core pupil record to ensure confidentiality and restricted accessibility.

Staff Records

Records relating to the Trust workforce will be held securely, either electronically or in paper format, with appropriate measures in place to ensure accessibility is restricted.

Storage and Security

All records, especially where containing personal data, will be stored securely to maintain confidentiality, whilst also keeping information accessible to those authorised to see it. Electronic records will have appropriate security and access controls in place, and systems will have robust audit functions in place wherever possible.

Paper records will be stored in secure, lockable storage areas with restricted access.

When sharing or transferring records containing personal information, we will ensure appropriate transmission security controls are in place, in line with our Information Security Policy.

Retention and Disposal

Retention is the period a record is kept for after it stops being actively used, but before it is destroyed. Retention is a vital part of records management as it allows organisations to retain records only for as long as needed, and discourages records being kept for long periods 'just in case'.

The retention period for particular types of records is determined by legal, regulatory or functional requirements. We have adopted a Retention Schedule based on the IRMS Schools Toolkit which sets out our specified retention periods.

We will ensure that any records containing personal or confidential information are disposed of appropriately and securely when they have reached the end of their retention period, in line with our retention schedule.

Records held in databases or electronic management systems with the functionality for automatic destruction of records after a specified period of time will be used wherever possible. A review of the records will be carried out prior to destruction, where practical.

Where automatic disposal is not in place, for example for paper records, we will carry out a manual review, at least annually, to ensure they are deleted in line with retention guidelines.

The disposal of all information is documented to ensure that we maintain a record of when it has been deleted and by whom. This allows us to evidence that a record no longer exists, or has been transferred to another institution, in the event of a subject access or Freedom of Information request being received.

Archiving

Records containing personal information will only be selected for archive with appropriate safeguards in place to protect the rights and freedoms of individuals. This will include anonymisation or pseudonymisation wherever possible.

Training

Since all employees are involved in creating, maintaining and using records, it is vital that everyone understands their record management responsibilities as set out in this policy. We will ensure that staff are appropriately trained or experienced and that they understand the need for effective record keeping.

When we introduce new technology or ICT systems, we ensure that users are appropriately trained to use these systems and can manage records within them effectively.

THIS POLICY IS WAITING FOR TRUST APPROVAL IN MARCH 2025

Date of last approval/revision	January 2025
Review interval (years)	3 Years
Responsible Officer	Director of Operations
Approval/Review bodies	CET Team/ Trustees
Trust approval date	
Date of next review	SharePoint