The Active Learning Trust

RECORDS MANAGEMENT POLICY

This policy is reviewed every two years

History of Document

Issue No	Author/Owner	Date Reviewed	Date Approved by Trust Board	Comments
1	DPO	June 2018	12 July 2018	1st formal issue
2	DPO	December 2018	13 December 2018	Minor amendment to 4.4

1. INTRODUCTION

1.1 Information is a key asset of the Active Learning Trust ("Trust") and it and its constituent academies create, receive and handle vast amounts of it. It is vital that the best use is made of this asset through effective policies and procedures, to inform decision making, improve accountability, and enhance services to students. This means having a consistent view on how Information is managed, created, stored, retrieved, retained, disposed of and shared.

1.2 By efficiently managing its records, the Trust will be able to comply with its legal and regulatory obligations and ensure effective management of its schools.

2. PURPOSE OF THE POLICY

2.1 This Records Management Policy ("Policy") outlines how records should be stored, accessed, monitored, retained and disposed of, in order to meet the Trust's statutory requirements.

2.2 This Policy takes into account the series of guides held by the National Archives which cover records management - Guidance

3. SCOPE

3.1 This Policy applies to all records created, received, maintained, used, distributed, shared, stored and disposed by staff of the Trust and its constituent academies in the course of carrying out its functions.

4. RESPONSIBILITIES

4.1 The Trust Board has ultimate responsibility for setting this Policy.

4.2 Headteachers are responsible for ensuring this Policy is implemented at their own school. Where the term Headteacher is used this incorporates Executive Headteacher roles where these exist and the Chief Executive Officer of the Active Learning Trust when the statement refers to the central Trust.

4.3 Individual members of staff should ensure that records, for which they are responsible, are maintained and disposed of in accordance with this Policy.

4.4 An Information Governance Working Group reports to the Trust's Senior Leadership Team and considers records management matters.

4.5 The Trust's Data Protection Officer is responsible for providing guidance and advice on good records management practice.

5. LEGAL FRAMEWORK/GUIDANCE AND POLICIES

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

5.1.1 Data Protection Act (2018)
5.1.2 General Data Protection Regulation (2016)
5.1.3 Freedom of Information Act (2000)
5.1.4 Limitation Act 1980 (as amended by the Limitation Amendment Act (1980)
5.1.5 Copyright, Designs and Patents Act (1988)

5.2 This Policy also has due regard to the following guidance:

5.2.1 Information Records Management Society "Information Management Toolkit for Schools" (2016)

5.3 This Policy will be implemented in accordance with the following Trust policies and associated procedures:

5.3.1 Data Protection Policy
5.3.2 Freedom of Information Policy and Publication Scheme
5.3.3 ICT Security Policy
5.3.4 Records Retention Policy
5.3.5 Data Sharing Policy
5.3.6 Information Governance Policy
5.3.7 Subject Access Request Policy

6. WHAT IS A RECORD

6.1 ISO 15489 standard for the management of records, defines a record as: "Information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business." Essentially, it is a record of the Trust's business that requires effective management and preservation. Examples of records include:

6.1.1 Correspondence;
6.1.2 Education records; and
6.1.3 Minutes of meetings.

6.2 A non-record, by definition, is an item of information that does not require the same rigour of management as that required for records and is of immediate value only. Non-records will be disposed of once they have served their useful purpose.

7. PUPIL RECORDS

7.1 Pupil records are specific documents that are used throughout a pupil's time in the education system – they are passed to each school that a pupil attends and includes all personal information relating to them, e.g. date of birth, home address, as well as their progress and achievement.

7.2 Hard copies of disclosures and reports relating to child protection/Child in Need /Early Help are stored in a separate pupil file stored in a securely locked filing cabinet in the Designated Safeguarding Lead's, Headteacher's or Inclusion Office.

8. STAFF RECORDS

8.1 Staff records are specific documents that are used throughout a person's time whilst employed by the Trust and includes all personal information relating to them, e.g. application form and contract of employment, qualification certificates and evidence to support entries on a school's Single Central Record.

9. RECORD MANAGEMENT LIFECYLE

9.1 Records Management is the process by which the Active Learning Trust ("Trust") manages all the aspects of records whether internally or externally generated and in any format or media type. All information goes through a lifecycle, from its creation to its disposal as follows:

9.1.1 *Pre-creation* – deciding what information needs to be captured as a record and how;

9.1.2 *Create/receive* – information that needs to be kept as a record can enter the Trust in many ways. Some is created within; some comes from external sources;

9.1.3 *Index/classify* – the addition of descriptive information to records to make them easier to find, manage the different versions, and show the level of protection required and the date on which disposal should be considered;

9.1.4 *Process* – records may need to be processed at any point (have something done to them) in order to achieve the Trust's business aims;

9.1.5 *Store/manage* – identifying whether records are electronic or physical and how/where they should be stored to preserve integrity and authenticity and so they are secure but can be efficiently accessed by those who need to use them and are authorised to do so. Active records are those requiring frequent access and they should generally be stored electronically in the immediate workplace. Inactive records requiring infrequent access should generally be stored elsewhere in a school or in another location;

9.1.6 *Retrieval* - the finding of stored records by those who are entitled to search for them.

9.1.7 *Destroy or Preserve* – if records do not need to be retained permanently, have outlived any business or statutory requirement to retain further and have reached the disposal date, they should be destroyed.

9.2 Good records management has several benefits:

9.2.1 Provides compliance with information legislation;

9.2.2 Provides effective evidence for demonstrating performance and accountability;

9.2.3 Ensures that the Trust conducts itself in an efficient and accountable manner:

9.2.3.1 efficient use of staff time (saving time searching for records).
9.2.3.2 efficient use of physical and virtual space.

9.2.4 Support and document policy formation and decision making.

10. RECORDS STORAGE

10.1 When records are created or received they should be held in files - these may be paper based or held electronically in shared directories, databases or document management systems.

10.2 The files should be organised in a structured way and have some indication as to their contents and relevance:

10.2.1 A front file cover for paper records stating the contents of the file;

10.2.2 A standard way of naming records;

10.2.3 Page numbering to show the page number and number of pages;

10.2.4 Only commonly known abbreviations should be used;

10.2.5 Issue control;

10.2.6 A means of showing that the record contains personal or sensitive Information;

10.2.7 Who is permitted to access the record;

10.2.8 Name of author;

10.2.9 Multiple versions / copies of the same data should not be stored;

10.2.10 Creation date or receipt date/ revision date;

10.2.11 Retention period, the date on which disposal and the action that should be taken; and

10.2.12 Storage location.

10.3 Where there are confidentially issues, files may be held in a secure storage area, on a computer or email box however colleagues with appropriate permissions should be able to access them in an employee's absence.

10.4 There should be valid reasons for keeping records which include but are not limited to:

10.4.1 There is a legal requirement to keep the information;

10.4.2 The information is needed to carry out the Trust's everyday business;

10.4.3 The information is for financial purposes;

10.4.4 Information is held which explains why and how a particular decision was made;

10.4.5 The information is needed if a decision is challenged; and

10.4.6 Information is publicly accountable.

10.5 For most data, there should be one lead copy. This will be the file of the person or department in a school which has the lead on the topic concerned. Other members of staff may also have a file on the same subject, but they should keep this only for so long as per the Trust's Records Retention Policy.

10.6 Storage of electronic held data must follow the Trust's ICT Security Policy.

11. SECURITY AND ACCESS

11.1 File/folder permissions and access rights must be established to ensure that they can only be accessed by the people with the right to do so. This requires controls including:

11.1.1 Procedures to document access to personal or confidential records;

11.1.2 Employees being aware of the types of information they can access for their roles;

11.1.3 Regular reviews will be undertaken of who has access to personal and confidential records with amendments to access where necessary;

11.1.4 Employees not accessing or creating personal or confidential records on mobile devices, unless these devices are approved by the Trust and are either encrypted or have a secure workspace.

12. BACK-UPs

12.1 Each school will conduct a back-up of information in line with the Trust's ICT Security Policy and IT Standards to ensure that all data can still be accessed in the event of a security breach, e.g. a virus, and prevent any loss or theft of data.

13. SHARING RECORDS

13.1 Before sharing data, staff must ensure that the requirements of the Trust's Data Sharing Policy have been met which include:

13.1.1 Consent has been obtained from data subjects to share it (unless there is a legal requirement to share);

13.1.2 Adequate security is in place to protect it; and

13.1.3 The data recipient has been outlined in a privacy notice.

14. CONFIDENTIAL RECORDS

14.1 These records should be labelled as 'Confidential' and be clear as to who within a school should be able to access and use these records. It is also good practice for the record to hold an intended publication date;

14.2 Confidential records should be stored in secure filing cabinets which should always be kept locked when not in use, not located in a public area, and access to the confidential records should be restricted only to those employees that require the information.

14.3 Confidential records should never be left in a public open area such as an in-tray or on a desk. The record should be returned to the cabinet when not in use.

14.4 For electronic records, confidential records should be held in separate directories or files with restricted access to these directories or files.

14.5 Laptops that hold confidential information must be Trust owned and encrypted by a school's IT service.

14.6 Confidential information should not be copied to non-Trust equipment.

14.7 Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of a school containing sensitive information are to be supervised at all times.

14.8 Confidential records must be destroyed by shredding.

15. EMAILS AND ATTACHMENTS

15.1 E-mails may be disclosed in response to a Freedom of Information or Subject Access Request and in legal cases. Electronic messages can be legally binding, and the Trust may be held liable for defamatory statements in e-mails. For these reasons, nothing should be recorded in emails that a person would not say in other forms of communication.

15.2 If an e-mail contains important information or an important decision, it should be added to the relevant file/folder either electronically or a hard copy. An email can be saved electronically using 'File – Save as - File'.

15.3 The Trust has an Email Acceptable Use Policy which outlines the framework of acceptable email usage and controls in order to safeguard information assets from unauthorised access and accidental or intentional damage.

16. RETENTION OF ARCHIVED RECORDS

16.1 Former pupil records held by a Sixth Form, accounting and personnel records, and some other records, will be archived until being disposed of. This does not include safeguarding files which are currently held by a Sixth Form indefinitely.

16.2 Archived records should be treated as being as confidential as current records. However, they should not necessarily be as accessible as current records but should still be retrievable.

16.3 Documents should be retained in accordance with the Trust's Records Retention Policy.

16.4 Electronic files can be archived by creating an archive subfolder on a Trust network drive. Within the archive sub-folder there would be folders named 'do not dispose until ….. '. This will make it easier to dispose of the archived records when they reach their destruction date.

16.5 Hard copy documents and files need to be prepared prior to being put into an archive storage box. Files should be removed from lever arch files and placed into card wallets/files and all metal removed as over time metal components may damage files.

16.6 The documentation should be reviewed prior to being placed in storage boxes to remove and destroy any paperwork that is not required to be stored i.e. duplicate items etc.

16.7 Archive boxes should be numbered and have an index of their contents together with the date that the contents should be securely destroyed. Such contents should also be recorded in a summary such as an excel spreadsheet.

17. PERSONAL DATA HELD BY THIRD PARTIES

17.1 When a contract has ended with a third party which processed personal data provided by the Trust, a check should be made as to the length of time the third party will retain the personal data before arranging for its secure disposal. Some organisations require notification by the Trust to dispose of personal data held on their systems and back-ups or allow an earlier disposal than recorded on their retention schedule upon written request from the Trust.

18. TRANSFER OF PUPIL RECORDS

18.1 Each school will, wherever possible, avoid sending a pupil record by normal post.

18.2 Where a pupil record must be sent by post to a new school, it should be sent by recorded post, with an accompanying list of the files included. The new school will be required to sign a copy of the list to indicate that they have received the files and return this to the school.

18.3 For safeguarding files where posted, such should be double enveloped and marked for the attention of the recipient school's Designated Safeguarding Lead. Personal data can also be transferred electronically via secure file transfer on the MyConcern software.

18.4 Pupil files can be delivered by hand if schools are situated locally and signed for by the receipting school. A pupil's safeguarding file and pupil record must not be combined when transferred to a new school.

19. DISPOSAL OF RECORDS

19.1 When faced with a decision about the disposal of an individual document, the following should be asked:

19.1.1 Has the information come to the end of its useful life?

19.1.2 Is there a legal requirement to keep this information or document for a set period?

19.1.3 Would the information be likely to be needed in the case of any legal proceedings? In particular, is it potentially relevant to an historic child abuse enquiry? (Is the information contentious, does it relate to an incident that could potentially give rise to proceedings?)

19.1.4 Would the document be useful for the organisation as a precedent, learning document, or for performance management processes?

19.1.5 Is the document of historic or statistical significance?

19.2 Confidential waste and documents with personal data should either be securely shredded on site or securely stored in confidential waste bins or sacks located in a locked office until collected for secure destruction by an accredited third-party processor.

19.3 Other documentation can be deleted or placed in recycling bins where appropriate.

19.4 In accordance with the Trust's Records Retention Policy and point 16.7 above, a list of hard copy records to be destroyed in bulk at the end of a retention period must be maintained and should include the name of the authorising officer and the date that that the documents were removed from archives to be destroyed. A suggested template is shown at Appendix I.

20. REPORTING

20.1 The Trust's Data Protection Officer is responsible for submitting a report on the effectiveness of this Policy to the Trust Board as a minimum on every two years.

21. REVIEW

21.1 This policy will be reviewed every two years by the Trust Board.

Appendix I

BULK DELETION OF RECORDS

Date	Type of Record	Year of records (if appropriate	Box No (if appropriate)	Date when contents are to be destroyed.	Date when contents were removed from archives for secure destruction	Authorisation to delete – signature or name of authoriser