Chatsworth Multi Academy Trust
Achieving Excellence Together

Chatsworth MAT Records Management Policy

This policy applies to all employees, governors and trustees including temporary, contract staff and anyone who undertakes work on behalf of Chatsworth Multi-Academy Trust regardless of their location. It applies to all records that are created, received and maintained by the school and its staff as evidence and information relating to school activities.

Version: 2

Reviewed: February 2023
To be reviewed: February 2024 or before if changes in law

Document control
Version control/History

Name	Description	Date
Andrew van Damms	V1.0 Records Management policy for schools	31/08/18
Debbie McCarron	V2 reviewed & updated references to UK GDPR	Feb 21

Approvals

Name	Position	Date

1. Introduction

Chatsworth Multi-Academy Trust ('the trust) recognises that efficient and effective records management is essential not only to ensure compliance with legal and regulatory obligations but the successful overall management of the institution. Records provide evidence for protecting the legal rights and interests of the school and provide evidence for demonstrating performance and accountability.

The trust holds a wealth of information in a variety of forms. This information is an important corporate asset that must be managed well in order to:

- Support staff in the effective and efficient conduct of trust business
- Contribute to the trust's overall management and governance
- Comply with its legal and regulatory obligations
- Support evidence-based decision making (transparency and accountability)

2. Definitions and scope of policy

Information can be defined as definite knowledge acquired or supplied about something or somebody. A **record** is made up of related pieces of information recorded as evidence of an activity. Records need to be accurate, reliable and available to ensure their validity. Examples of records held by the trust include:

- Pupil records
- An invoice for goods or services received
- Minutes of a meeting
- Information regarding entitlement to free school meals
- Parent/guardian/carer contact information

Records management is about controlling records throughout their lifecycle; from creation/receipt until their eventual destruction or preservation. Records must be identified, classified, stored, secured and tracked in order to manage them efficiently.

A record can be in any format, e.g. paper, electronic, photograph, voice/sound recording, and microfiche. It can be stored on any medium and/or in any facility, e.g. paper, on-site and off-site storage, within a computer system, on a network drive. Both originals and copies are classed as records.

Email systems are a means of transporting/sharing information and should not be used as a record storage area. **Email messages (and any attachments) are temporary files** until they are stored outside of the email system, for instance, in a network folder or business system.

In terms of this policy, 'records' are defined as all documented information relating to the business of the trust which has been created, received, and maintained by staff of the trust for the performance of trust functions.

The policy applies to the management of trust records regardless of format or the location from or in which trust employees, agents, contractors and partners access them.

3. Responsibilities

The Board of Trustees 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 on a day-to-day basis is the school's Head Teacher and the college's Vice Principal.

Internal control systems and procedures will be subject to regular review to ensure they provide an effective framework for the management of the full lifecycle of trust records i.e. creation, maintenance and disposal/destruction.

The school/college's leadership are responsible for ensuring that those reporting to them are made aware of and understand this Policy and are given adequate and regular training on it. Training may also be provided through the council's Information Governance SLA service.

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

4. The Regulatory and legislative environment

The activities of the trust are governed by a comprehensive and complex legal and regulatory environment. **Failure to appropriately manage records can lead to significant financial penalties and other types of regulatory intervention e.g. enforcement action.** Key legislation, regulations and codes of practice governing the way the trust manages its records and information include:

- UK General Data Protection Regulation
- Data Protection Act 2018
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Criminal Justice Act 1988
- Civil Evidence Act 1995
- Regulation of Investigatory Powers Act 2000
- Human Rights Act 1998
- Re-use of Public Sector Information Regulations 2015
- Code of Practice on Records Management issued in July 2009 by the Lord Chancellor under section 46 of the Freedom of Information Act 2000
- Local Government Transparency Code 2015.

The trust will have regard to authoritative practice guidance, incorporating it as appropriate into its records management arrangements. Key sources include The Information Records Management Society (IRMS, the Information Commissioner's Office (ICO), and the Department for Education (DfE).

5. Records Management

To properly manage records, the records lifecycle must be understood. Records management is about placing controls around each stage of a record's lifecycle, from the point of its creation (or receipt), during its use, to its ultimate destruction or permanent preservation.

Creation/ Receipt	Every record should be classified when it is created (or received), as this will determine how it is managed throughout its lifecycle. Information the trust holds will generally be categorised as either **unrestricted** and **controlled access information** **Controlled access information -** needs to be restricted to specified groups/individuals who are authorised to access it. Examples include personal data (special category or otherwise), pupil data **Unrestricted –** access does not need to be restricted as there is no valid reason (as per above).
Usage/ Storage	How, where, by whom and for how long will the record be in use? **Access**: this must be appropriate to the category of the information i.e. records containing controlled access information must be restricted to authorised users, including off-site storage. The primary copy of a 'live' record must be readily available and should be stored in a trust network folder or system. Personal folders/devices should not be used for trust records that need to be accessed by colleagues. **Location**: records must be appropriately secured regardless of where the information is in use – on-site or off-site. Controlled access information must never be stored on an unencrypted device, e.g. pen drive, CD. Original records should never be moved off the trust's network/premises – if they are needed off-site, copies should be made, to minimise the risk of loss **Sharing**: controlled access information must only be shared where there is a business case or a legal basis to do so, and it must always be encrypted in transit, e.g. when sent by email or copied onto a removable device **Retention**: Legislation and business practices will specify how long different types of records need to be kept
Archive/ Permanent Preservation/ Disposal	The retention period determines what happens when a record is no longer live. **Archive**: records that need to be retained for a long period of time, but are no longer in use, should be archived. **Permanent Preservation**: records that will never be destroyed, to protect and make available the corporate memory of the organisation to all stakeholders and for future generations. For example, property deeds, birth certificates etc. **Disposal**: the permanent destruction of records. Records containing controlled access information must be securely disposed of, e.g. paper must be securely shredded, electronic media must be crushed/rendered unusable

6. Data Quality

Records are only as good as the information they contain – so they must be accurate, reliable and available. Inaccuracies, duplicates and misplaced records cause misinformation.

Accuracy: when creating and amending records, all information must be checked for accuracy before saving. For example, an incorrect address could result in information being sent to a third party.

Reliability: incomplete information cannot be relied upon. For example, don't create a new record for Maggie Jennings if one already exists for Margaret Jennings. Make checks to see if they are the same person first, as separate records would give to an incomplete picture.

Availability: information needs to be accessible in order to ensure the effective operation and administration of trust business. For example, work records stored in an employee's personal folder would not be accessible to colleagues, who may need to access them in the event of absence.

7. Record Retention

Retention – the length of time that records are kept – must be managed as it can be costly, inefficient and, in some cases, illegal to keep records longer than necessary.

- Storage space costs money – in terms of IT disk space and/or off-site storage of physical records
- The more records held, the longer it takes to find the information that is needed
- Data protection legislation states that personal data should only be kept for as long as necessary to support the purpose for which it was collected.

A record Retention Schedule has been created.

Retention periods are determined either by specific legal requirements, 'industry' and best practice recommendations issued by government departments e.g. DfE, appropriate advisory bodies, e.g. IRMS, or otherwise business needs determined by the trust.

It is important that all applicable retention criteria are considered to ensure that any retention/disposal does not compromise the trust's ability to meet its business or legal requirements.

It is possible that a record may have more than one retention period because it is used in different ways. The information may serve a purpose other than that it was created for e.g. it may need to be kept as part of an investigation. In any case, the longest retention period would apply.

8. Record Disposal

Records should be regularly reviewed (at least annually) to identify those that have reached the end of their useful life/retention period (whichever applies) and are due for disposal. Those identified should be reviewed before being disposed of to ensure that they are not required as part of a current investigation, e.g. HR disciplinary or a request for information. **If this is the case, disposal must be postponed until the needs of the request or investigation have been satisfied or in cases of non-disclosure/complaint, until an**

appeals procedure has been exhausted. Unless there is specified requirement, all copies of records due for disposal should be destroyed.

Physical records classed as controlled access information **must be securely shredded**. This will incorporate all records containing personal data. These records must be stored securely while awaiting disposal

Electronic media used to store controlled access information must be securely destroyed at the end of its useful life, e.g. computer hard drive, USB memory stick.

Unrestricted paper records may be recycled or disposed of through normal waste collection services.

Records identified as being of permanent value should be transferred to an appropriate archive.

9. Archiving

Where the trust identifies records as being of permanent value i.e. for archiving/ historical research, they should be transferred to an appropriate archive. Advice can be sought from the Council and Salford Local History Library (run by Salford Community Leisure) as to how to manage the process.

A database of the records sent to the archives is maintained by the Trust Business Manager. The appropriate staff member, when archiving documents should record in this list the following information: -

- File reference (or other unique identifier);
- File title/description;
- Number of files; and
- Name of the authorising officer.

10. Monitoring Arrangements

The Headteacher and Vice Principal is responsible for monitoring compliance with this policy. Failure to adhere to this policy may result in breaches of legislation and affect the trust's ability to deliver its services and to demonstrate that it is open and accountable.

The policy template will be reviewed annually and updated if necessary as part of the IG SLA.

The trust will ensure that all staff are aware of and have read this policy.