RECORDS MANAGEMENT POLICY

Resilience Multi Academy Trust

Summary	Records Management Policy		
Responsible Person/Author:	COO		
Applies to: (please circle/delete as appropriate)	**Colleagues ☒**	**Student☒**	**Community ☐**
Ratifying Committee(s)	Trust Board		
Available On:	SharePoint, On Demand		
Date of Approval	27 April 2026		
Effective from:	28 April 2026		
Date of Next Formal Review:	July 2028		
Review Period	2 Years		
Status:	Non-Statutory		
Owner	RMAT		
Version:	5		

Document Control

Date	Version	Action	Amendments
30.03.26	5	Amendments	Para 2 – Ref to code of practice and FOIA. Para 8- Definition of record. Para 12 – Ref to information manager. Para 13 – Ref to functional leads. Para 38 – Ref to essential info. Para 45 – Ref to last known school. Para 53 – Ref to annual data audits. Para 56 – Ref to FOI and SAR responses. Para 82 - Digital continuity metadata and file naming section added. Para 83 – Cloud storage section added. Para 84 – Use of AI and automated processing added. Para 95 – Ref to destruction log added.

			Para 97 – Ref to need to comply with BSEN15813 added. Para 102 – Ref to secure deletion. Table 1/29 – Ref to Restrictive intervention record and CSA. Table 35 – Digital and electronic records added

Contents

Records Management Retention Tables

Introduction

1. RMAT 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 RMAT. Records provide evidence for protecting the legal rights and interests of RMAT and provide evidence for demonstrating performance and accountability.

2. This policy aligns with the Lord Chancellor's 2021 Code of Practice on the Management of Records issued under Section 46 of the Freedom of Information Act 2000. Records must be managed as evidence or as information assets that support business activity ensuring authenticity, reliability, integrity and usability.

3. This policy provides the framework to achieve effective management and audit of records.

4. The security of data and appropriate measures will be implemented to protect, breach, loss or unauthorised sharing of information.

5. Information will be assessed as to when it is no longer required, necessary, or is to be destroyed or deleted in line with the retention schedule.

Scope of the Policy

6. The policy applies to all records created, received, or maintained by permanent and temporary colleagues, agents, contractors, consultants or third parties acting on behalf of RMAT while conducting their functions.

7. Records are defined as all those documents which facilitate the business conducted by RMAT and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received, or maintained in hard copy or electronic format.

8. A record is any information created, received, or maintained as evidence of an activity or as an information asset. Information of no evidential or operational value must not be treated as a record.

Publication of this Policy

9. This policy will be available to all colleagues, members of Trust Governance and members of the public and will be available to them as needed. Guidance on any aspect of this policy can be obtained from RMAT's Data Protection Officer ("DPO"). amarham@rmat.uk .

Responsibilities

10. The RMAT Board has a statutory responsibility to maintain RMAT records and recordkeeping systems in accordance with the regulatory environment specific to RMAT. Day to day management is delegated to the RMAT Executive and Academy Principals.

11. Academy Principals are responsible for guidance in their Academy on good records management and should promote compliance with this Policy, so that information will be

retrieved easily, appropriately and in a timely manner. Academy Principals should also annually survey records to check they are stored securely and can be accessed appropriately.

12. The DPO will act as RMAT's Information Manager responsible for oversight of records management practice, annual compliance checks and the maintenance of standards, procedures and guidance and undertakes a risk analysis to identify which records are vital to Trust and Academy management and these records will be stored in the most secure manner.

13. Functional leads remain responsible for destruction of records within their area.

14. RMAT will manage and document its records disposal process in line with the Records Retention Schedule. This will help to ensure that it can meet Freedom of Information Requests and respond to Subject Access Requests.

15. Individual colleagues must ensure, with respect to records for which they are responsible, that they:

    - Manage RMAT's records consistently in accordance with Trust policies and procedures.
    - Properly document their actions and decisions.
    - Hold personal information securely.
    - Only share personal information appropriately and do not disclose it to any unauthorised third party.
    - Dispose of records securely in accordance with the Academy's Records Retention Schedule.

16. Everyone who receives information in RMAT including Members, Trustees, LRB members, colleagues, contractors, and service providers has a duty of confidentiality and responsibility to safeguard Trust information or data that they access, regardless of the fact it may not be marked.

Aims of this Policy

17. To set out how RMAT will manage its Records.

18. To support the values of RMAT and its Academies.

Security Classification of RMAT Records

19. In 2018, the UK Government issued updated guidance on security classifications that the public sector should employ. This obliged that the public sector classifies information into 3 types:

    - Official
    - Secret
    - Top Secret

20. The Classification recognised that the public sector needs to collect, store, process, generate or share information to conduct business and the classification above would be reflective of risk.

21. Most information that is created and processed in the public sector is classified as Official. This classification applies to all Trust records. It reflects the routine business operations and services of RMAT and that if information is lost, stolen, or published in the media it could have damaging consequences for RMAT but will not be subject to a heightened threat profile.

22. As all information in RMAT is considered as Official, RMAT **does not** require it to be routinely marked. RMAT **does** require those who receive information in RMAT to comply with the information controls put in place. **All information must be managed with care to comply with legal and regulatory obligations to reduce the risk of loss or inappropriate access.**

Sensitive Information

23. Sensitive information should only be provided to a recipient based on a genuine **need to know** and that appropriate security controls are in place. Information in RMAT needs to be available to the right people at the right time with the intention that RMAT is as transparent as possible whilst considering data protection and confidentiality requirements.

24. Sensitive information should be considered as information which if lost, stolen, or published would have damaging consequences for RMAT. Such information should be marked **OFFICIAL – SENSITIVE**

Descriptors

25. Sensitive information in RMAT should also include 1 of the 2 following descriptors:

- **OFFICIAL SENSITIVE COMMERCIAL**

  This is commercial information of RMAT including that relates to its statutory or contractual obligations that may be damaging to RMAT or a commercial partner if improperly accessed.
  OR

- **OFFICIAL SENSITIVE PERSONAL**

  This is sensitive information relating to an identifiable individual where inappropriate access could have damaging consequences. Examples may include:

  - Investigations into colleagues.
  - SEND records.
  - Student or colleague medical records.

Marking Official Sensitive Information

26. Official Sensitive Information should always be marked. To ensure consistency across RMAT, they should be marked as follows:

- The top or bottom of documents in the middle of the header.
- The subject line or body of emails or
- The front of folders or binders.

Security Outcomes

27. All Trust information must be managed with care to prevent loss or inappropriate access. To deter this RMAT will deter deliberate compromise or opportunist attack.

28. RMAT will employ the following controls to achieve the outcome detailed above.

Personnel Security	Access by authorised individuals for legitimate business reasons.
Physical Security	• Proportionate good practice precautions against accidental or opportunistic compromise. • Control access to sensitive assets through Trust processes and dispose of with care to make reconstitution unlikely.
Information Security	• Protect against deliberate compromise by automated or opportunist attack. • Aim to detect actual or attempted compromise and respond.

29. RMAT will also employ the following controls:

Personnel Security	• Appropriate recruitment checks • Need to know for sensitive information
Document handling	• Clear desk/screen policy
Storage	• Storage under single barrier and/or lock and key • Use of appropriate physical security equipment. E.g., lockable filing cabinet
Moving records by hand	• Ensure cannot be overlooked when working in transit
Moving records by post	• Use Royal Mail or a reputable courier's track and trace service.
Moving records electronically	• Sensitive records should be transferred securely using appropriate encryption
Removable media	• Should not be used on Trust devices.
Providing information on the Telephone	• Caller ID should be verified including the telephone number they are calling from, and security questions answered.
Disclosure under an FOI or SAR	• These should only be disclosed with the express consent of RMAT Data Protection Officer.

Student Records

30. RMAT is under a duty to maintain a student record for each student. The student record comprises the educational and curricula record of each student and is the core record charting the individual student's progress through the education system and accompanies the student through their school career. It is the formal record of their academic achievements, other skills and abilities and progress in their Academy.

31. Student Records held in RMAT are a mixture of records held in paper form and electronically such as part of the School Information Management System. All information must be easy to find, accurately and objectively recorded and expressed in a professional manner. Colleagues are reminded that Students and Parents have a right of access to their educational record via the **Data Protection Act 2018** ("DPA") and the **UK General Data Protection Regulation** ("GDPR"). RMAT treats requests for information from students or parents as requests under Data Protection legislation.

Paper Files

32. The following information should be placed on the **front cover** of a Paper student file:

- Surname and Forename
- Date of Birth
- Unique Student Number
- Date file was started.

Paper Files or School Information Management System ("SIMS")

33. The following information should be **inside the front cover** of a Paper student file or should be held on **SIMS**:

- Emergency contact details.
- Preferred name.
- Name and contact details of adults who have parental responsibility and/or care of the student.
- Reference to further information held on allergies.
- Reference to further information held on medical conditions.
- Other agency involvement e.g., Special Educational Needs and Disabilities ("SEND") or speech and language therapist; and
- References to any other linked files.

Other Items to be included on Student Files:

34. The following items should also be held on the Student File:

- Admission form.
- Current Data collection/checking form.
- Annual written report to parents.
- Information relating to a major incident involving the student.

- Information relating to a Fixed Term Exclusion.
- Information relating to a Permanent Exclusion.
- Specific correspondence with parents or outside agencies relating to a major incident. This may be in e-mail form. Once the matter is closed, save any correspondence that records events, pertinent issues, and outcomes to student record.
- Summary details of complaints made by a parent or the student relevant to the student's ongoing education/behaviour. Again, this may be in e-mail form. Once the matter is closed, save any correspondence that records events, pertinent issues, and outcomes to student record.
- Student copy of Examination results. Uncollected certificates should be returned to the Exam board after all reasonable efforts to contact the student have been exhausted.

Items to be kept in a separate area of the record or kept in a separate linked file:

- Educational support plans and statements in support e.g., SEND or speech an
- Medical information relevant to the student's ongoing education/behaviour.

Items to be kept in a separate area of the record or kept in a separate linked file to limit access to specific colleagues:

- Child protection reports.
- Child protection disclosures; and
- Child protection supporting documentation.

Records not forming part of the Student Record

35. The following records should be stored separately from the student record as they are subject to shorter retention periods **and should not be forwarded to any school the student moves to:**

- Attendance registers and information.
- Authorised Absence notes and correspondence.
- Parental consent forms for Excursions.
- Accident forms (a copy can be placed on the student record if it is a major incident).
- Medicine consent and administering records.
- Copies of birth certificates, passports etc.
- Generic correspondence with parents about minor issues (i.e., Dear Parent).
- Student work.
- Previous data collection forms which have been superseded. These should be destroyed.
- Photography/Image consents

Transfer of Student Records

36. Student Records should be transferred to any school that a student moves to as soon as possible to ensure decisions can be made about a student using relevant and accurate information. The Record should **not** be weeded before transferring other than duplicates or records with a shorter retention period which should already have been disposed of.

Transfer Process

37. Student Records should be transferred within 15 school days of receipt of confirmation that a student is registered at another school:

- Common Transfer File should transfer SIMS information together with SEN or other support services information which is on SIMS.
- Child protection information should be sent as soon as possible by the Designated Safeguarding Lead or a member of their team to an equivalent person in the new school.
- Any other electronic records should be transferred to a named contact at the other school via secure encrypted email or other secure transfer method.

38. In addition to statutory transfer, RMAT will share limited essential information earlier where necessary to ensure continuity of safeguarding and SEND provision. This may occur shortly after National Offer Day using Public Task or Recognised Legitimate Interests as the lawful basis. Receiving schools must destroy information if the pupil does not enrol.

Independent School or a Post 16 Establishment

39. If a student is transferring to an Independent School or Post 16 establishment, a copy file should be transferred and the student file should be retained as the current Academy will be the last known mainstream school.

Transfer outside of the UK

40. If a request is made to transfer a student file outside of the UK, colleagues considering the request should contact the Data Protection Officer for further guidance.

Retention of Records Post Transfer

41. Following Transfer, Academies should retain information about a student for a short period to allow for any queries or reports to be completed or where linked records have not yet reached their retention period and deletion would cause problems.

42. Elements of records may need to be retained for longer for example if litigation is pending. Academy Principals should discuss any such records with the Data Protection Officer.

43. All child protection files should be retained.

Last Known Academy

44. Academies are responsible for retaining the student record for all students who:

- Have left at 16 years old.
- Where a student leaves for elective home education.
- They are missing in education; or
- They have left the UK.

45. The last known school retains the full student record for 25 years from date of birth. This includes safeguarding, SEND and incident records.

Information Audits

46. Information Audits allow RMAT to consider:

- What information is retained?
- Why is information retained?
- What type of information is?
- How information is processed and shared.
- Where is information stored?
- What the relevant retention period is?
- Who the information owners or day to day users are?

47. Information Audits will consider all information held regardless of its form and will include:

- Paper documents and records.
- Electronic documents and records.
- Databases.
- Microfilm/Microfiche.
- Video and Photographic files.
- Hybrid files and
- Apps and portals.

48. The information Audit will allow each Academy and RMAT to complete an Information Asset Register, which allows the capture of all knowledge in RMAT and the management of that knowledge in the same way other assets such as colleagues, buildings and money are managed.

49. Effective management of our Information allows the right information to be given to the right people at the right time.

50. The benefit of Information Audits are as follows:

- RMAT can manage information to get the most effective use from it.
- RMAT can more easily manage information considering its responsibilities under the DPA, GDPR and Freedom of Information ("FOI") Requests.
- It saves time.
- It avoids duplication.
- It helps ensure accuracy of information.
- It allows RMAT to demonstrate compliance with the DPA.

51. Information audits will be conducted by the DPO in conjunction with Academy Principals and/or Trust Central Services teams and may include:

- Interviews with colleagues with key responsibilities to identify information and information flows.
- Questionnaires distributed to key colleagues to identify information, information flows and so on; and
- A mixture of the above.

52. Information audits will include the following: -

- The Academy's/Team's data needs.
- The Information required to meet those needs.
- The format in which data is stored.
- Retention period for data.
- Vital records status and protective marking; and
- Maintenance of the original document.

53. Data audits must be conducted annually and fed directly into the Information Asset Register. All systems, paper stories, cloud platforms, and third-party vendor systems must be included.

54. Once the information is confirmed as accurate, the information will be included in the Information Asset Register which will be approved by the Academy Principal or Chief Executive as appropriate.

Electronic Communications Records Management

55. Content created and shared by messaging and discussion forums is usually temporary. If the content subsequently becomes more important (and is needed to be formally recorded such as evidence in a safeguarding case) then it should be copied and moved into an appropriate filing system either by saving it in a readable electronic format, printing it out or taking a screenshot.

56. Any content retained is held subject to the DPA and can be subject to FOI requests. This includes e-mails, instant messages, text, or message boards. Electronic communications stored in mailbox folders are not deleted until permanently removed. Deleted items remain within scope for FOI and SAR responses.

E-mail

57. When sending emails, ensure that the email is being sent to the correct recipient. If an email is being sent to multiple external recipients use the Bcc feature so that other recipients do not receive the email address of other external recipients.

58. A secure encrypted e-mail or data transfer system should only send confidential or sensitive information. A student's name or other personal information should never be put in the subject heading.

59. Email should not be used as a filing system storing information that should be stored somewhere else. If needed emails and attachments should either be saved in an electronic filing system or printed and placed on a paper file.

60. When considering whether to retain an email and its attachment, colleagues should consider whether it forms part of a student's record, is part of a contract or relates to an employee. This allows the email to be retained in line with the respective retention period for the type of record.

61. RMAT intends that emails should be deleted from a user's inbox after 6 months. Employees who leave RMAT should have their emails placed on divert to a suitable remaining employee for 6 months after their departure before the inbox is deleted. Members of Trust Governance who leave RMAT should have their user inbox immediately deleted.

Faxes

62. If a colleague is sending confidential information by fax, the colleague should check the recipient is correct before sending the fax.

Microsoft Teams

63. Colleagues, students, and members of Trust Governance who use Microsoft Teams should think about who will see any information posted on Teams. Recorded information on Teams is subject to Data Protection and can be the subject of a Freedom of Information request.

Use of Personal devices

64. If colleagues or members of Trust Governance access emails or Microsoft Teams on personal devices they should contact their IT helpdesk for configuring the device, encryption, and password protection.

Social Media Records Management

65. Where personal data such as images, names or other personal data is published on social media, it must only be done with the consent of a parent/student. The consent should be clear and unambiguous including where the information will be shared and for how long.

66. Any colleague who is responsible for a social media account should familiarise themselves with the account's retention period. Before publishing any item on social media, colleagues should be aware that once something has been posted it can be shared, liked, or commented upon in a way that was not originally intended.

67. Social media posts can be the subject of a freedom of information or subject access request.

Digital Continuity Statement

68. Any Digital record which needs to be preserved for 6 years or longer should be subject to a digital continuity statement. Appropriate records need to be identified as early in their life cycle as possible together with records which do not need a statement in the policy. A continuity statement should only be applied to principal copy records.

69. Digital records subject to a continuity statement should be usually archived to dedicated server space. If this is not possible the records should be transferred to high quality CD/DVD. If they are transferred to high quality CD/DVD they should be regularly checked for data degradation. All new storage methods should be discussed with the Data Protection Officer to ensure an appropriate statement is put in place where needed.

70. Flash drives may not store any record subject to a digital continuity statement as they are prone to corruption and can easily be lost or stolen.

71. Records subject to a Digital Continuity statement must be archived in an internationally recognised file format.

72. Digital continuity statements should include: -

- Statement of the purposes and statutory requirements to keeping records.
- A description of the business purposes for the information asset and the retention period for the records.
- A brief description of the consequences of loss.

73. Any continuity statement created should be provided to the Principal of the Academy or Chief Executive who is the Information Asset Owner and the Data Protection Officer who is responsible for long term data preservation.

Migration of electronic data

74. Where electronic data is required for longer than the lifespan of the system upon which it is held, the system specification should state the accepted formats for the storage of records within the system so that the system does not have to be retained for the lifespan of the data.

75. Any data transferred from the main system to an external storage device must be backed up and two secure copies of the data should be made. Data on the storage device and the backups should be checked regularly to ensure it is still accessible. Backups should be taken at least annually.

Storing and Protection of Information

Paper Records

76. Confidential Records should be kept in a locked filing cabinet, drawer or safe with restricted access. They should not be left unattended or in clear when held in a location with general access.

Electronic and Digital Records

77. Backed up information should be stored off the Academy premises to which it relates or the central back up function should be used.

78. Digital data should be coded, encrypted or password protected, both on any local hard drive or network drives.

79. Data should only be saved on removable or portable storage devices with the express permission of the Director of IT and Data. If it is such device should be kept in a locked filing cabinet, drawer or safe when not in use. Memory sticks should not be used in any Trust device.

80. Electronic devices must be password protected to protect the information on the device in case of theft. Where possible, Trust devices will be enabled to allow the remote blocking or deletion of data in the case of theft.

81. Colleagues and members of Trust Governance have their own secure login and password, with prompts used for changes of passwords.

Digital Continuity, Metadata and File Naming.

82. RMAT will maintain digital continuity for all records required for more than six years. Metadata standards must be applied to describe context, content and structure. Colleagues must use consistent file naming formats to support retrieval, for example: YY-MM-DD_Surname_title..docx.

Cloud storage and system procurement

83. Any system used to store records must allow secure deletion, export and migration without vendor lock in. A DPIA must assess whether data held in cloud systems can be fully deleted, including backups.

Use of AI and Automated Processing

84. RMAT will not use personal data to train AI models. Non-personal datasets may be used where anonymisation or pseudonymisation is applied in line with ICO guidance. AI may be used for classification, search and summarisations provided governance controls are in place.

Taking Records off RMAT Premises and Sharing Records

85. Where personal or confidential information is taken off Trust premises to fulfil the purposes of the data in accordance with GDPR, either in electronic or paper form, colleagues should take the same procedures they would do if accessing the information on Trust premises. Devices and paper records should be kept secure in a building and never left in a vehicle or on public transport.

86. Before sharing data, colleagues should ensure:

- Consent has been given from the data subject.
- Adequate security is in place to protect the data; and
- A suitable privacy notice applies to the recipient.

Limiting Access to Records

87. To prevent unauthorised access to records, colleagues should implement a 'clear desk policy' to avoid unauthorised access to physical records containing sensitive or personal information.

88. Under no circumstances should visitors be allowed access to confidential or personal information. Visitors to areas where sensitive information is stored should be always supervised.

89. Where an Academy is subject to vandalism, burglary, or theft, this should be reported to the DPO for additional security measures to be implemented.

90. Students/Parents or colleagues who request information held by RMAT about them should complete a Subject Access Request and the information should only be released on the authority of the DPO.

Safe Disposal of Records at the end of their Retention Period

Managing records retention

91. A principle of Data Protection is that Personal data must be kept for no longer than is necessary for the purposes for which it is processed. All records are therefore applied a retention period.

92. Disposal must be conducted in a timely manner to:

- Ensure compliance with legal retention requirements.
- Improve the efficiency of the recordkeeping system.
- Free up storage space.
- Reduce associated storage and management costs.

93. Destruction should include all backup and duplicate copies. Once an email has been moved into a records system, there is no need to retain the email as the information is available from the record system.

94. Destruction must be undertaken in a way that preserves confidentiality of information making it permanently unreadable and unable to be reconstructed or re-installed. Special care should be taken when destroying personal, sensitive, or commercial information and confidentiality should be paramount in all stages of the process.

95. RMAT must maintain a destruction log to demonstrate lawful deletion, including authorisation, method of destruction, and date. This is required to comply with FOIA Section 77 and Data Protection Act 2018 Section 173.

Destruction of Records by Type:

(1) Paper Records

96. Records containing personal data should be shredded. If an Academy employs a third-party contractor to shred papers, they should ensure that they are certified for the following: -

- BSEN15713: Secure destruction of confidential material.
- BS7858: Staff secure vetting.
- ISO 9001: Service Quality.
- ISO14001: Environmental Management Standard; and
- ISO 27001: Information security.

97. Confidential wate provides must comply with BSEN15713 for secure destruction of confidential material. For digital media, RMAT will follow NCSC secure sanitisation guidance.

98. It is also recommended that any third-party contractor is a member of one or more of the following organisations:

- British Security Industry Association.
- Federation Against Copyright Theft.
- Freight Transport Association.
- Fleet Operator Recognition Scheme.
- National Association for Information Destruction.
- Safe Contractor; and
- UK Security Shredding Association.

99. If any contractor is brought on site to provide secure shredding, Academies should ensure that they are supervised properly in line with Academy safeguarding policies. If an off-site shredder is chosen, Academies should ensure that they complete GDPR due diligence on the contractor and receive a Certificate of Destruction.

100. Any Certificate of Destruction should be retained with details of the records destroyed. Before Destruction takes place, confirmation should be obtained from the Information Asset Owner.

(2) Electronic and other media records

101. Electronic records should be routinely identified for deletion. Confirmation that the record can be deleted should be obtained from the Information Asset Owner who should only confirm deletion if:

- All legal and Academy requirements have expired.
- There is no related litigation or investigation which requires access to the records.
- Secure deletion can take place which includes backups and copies.

102. Secure deletion requires permanent erasure from all live systems, backups and replicas, or placement “beyond use” where full deletion is technically impossible.

103. If information is past its data retention period but cannot be permanently deleted from an electronic system, it should be put beyond use. Such information:

- Should not be used for any decision making or in a manner which affects an individual in any way.
- Not be given to any other organisation.
- Have appropriate technical and organisational security and access controls; and
- Become permanently deleted when this becomes possible.

104. Information put beyond use is exempt from subject access requests but may still need to be provided in response to a Court Order.

105. Deletion of Electronic records should only be undertaken with the agreement of the Information Asset Owner, the Data Protection Officer and the Director of IT and Data. The Director should advise on the method of deletion.

Transfer of Information to other media

106. If an Academy wishes to convert paper records into an alternative format such as microfilm or digital media, it should consider:

- The lifespan of the media and the ability to migrate data.
- Conversion should be done in a standardised fashion.
- That it can be evidenced that the electronic version is a genuine copy of the original and that the integrity of the data has not been compromised.

107. Original records should be retained for 6 months from the date of transfer to other media so that any issues arising out of the data transfer process must be identified.

108. If an Academy uses an outside contractor, they should ensure that the contractor is GDPR compliant and confirms to all security and staffing vetting requirements and have a data processing agreement in place.

Transfer of records to the Local Record Office

109. If an Academy concludes that a record is worthy of permanent preservation, arrangements should be made to transfer the record to the Local Record Office. This can either be done during the records active use or once the administrative use has been concluded. The Academy should ensure it considers access requirements and agrees this with the Local Records Office.

110. If records are transferred to the Local Record Office before the end of the records active use, they remain subject to the DPA and FOI Requests. Details of what has been transferred to the Local Record Office should be retained to enable identification for future use.

111. If an Academy decides to keep its Archive on site, they should take advice from the Local Record Office for specialist advice on storage and preservation requirements.

Documenting of all archiving, destruction, deletion, and digitisation of records

112. **The Freedom of Information Act** requires that a record must be kept of all records which have been destroyed together with who authorised their destruction, together with confirmation that the destruction took place as part of this records management policy.

113. A record should be made of all data destroyed, deleted, or transferred. It should contain:

- File reference or Unique Identifier.
- File title or brief description.
- Number of files or volumes.
- Date range.
- Reference to any applicable retention period.
- Name of the authorising officer.
- Date approved for disposal.
- Date destroyed or deleted from the system.
- Method of disposal.
- Place of disposal; and
- Person(s) who undertook destruction.

114. The record of destruction, deletion or transfer should be retained in the Academy office for Audit purposes.

Physical Storage of Records:

115. Records should be stored in a way that does not cause a health and safety hazard. They should not be stored in corridors or block or impede fire exits. They should be secured against intruders and there should be controlled access to the working space.

116. Records should not be stored under water pipes or in places liable to flooding. They should also be stored at least 2 inches off the ground to protect against immediate flooding. Records should not be stored in direct sunlight or areas of high humidity (above 65%).

117. Core records should be kept in cabinets or cupboards. Important core records should be stored in a fireproof cabinet. After use, records should be returned to their cabinet and not kept on desks or shelves.

118. Records storage areas should be kept clean and tidy and free of electrical equipment.

Retention Periods:

Student records and other student related information

119. Retention of all records relating to students should take into account the recommendations of the report of the Independent Inquiry into Child Sexual Abuse (IICSA). The report from the Inquiry recommended that records associated with child sexual abuse (CSA) should be preserved for 75 years. The Inquiry emphasised the need for this extended retention period

due to the significant value these records hold for victims, and advised that they should be subject to regular reviews throughout this duration.

120. In instances where there is evidence or allegations of CSA, schools and academies may decide to retain the complete record - whether of a student, colleague, or other related documents - not merely the segments directly related to the abuse.

121. The Inquiry report advised that the UK government instructs the Information Commissioner's Office (ICO) to develop a Code of Practice concerning the retention of, and access to, records known to relate to CSA. This has not been actioned some years following the report's publication, and it is unknown whether this work will be completed. Therefore, there is no statutory requirement to retain these records for such an extensive time period, and a careful management review will need to take place for each record where CSA is relevant before disposal or destruction of the record.

122. The Tables below outlines RMAT's retention period for individual student records and the action that should be taken after the retention period in line with any requirements. Electronic copies of information and files should also be destroyed in line with the retention period below:

Table 1- Student Records

Student's Educational Record		
File Description	**Retention Period**	**Action at end of Record**
Student's Educational Record	Date of Birth of student plus 25 years	Secure Disposal
Exclusion Records		
Restrictive Intervention Record		
Examination Registrations	Mandated by Exam Board	
Student copies of Exam Results: • Public • Internal	Information added to student record	All uncollected exam certificates should be returned to the Exam Board
Child Protection Information held on student file	Child Protection records on the student file should be in a sealed envelope on the student file.	Secure Disposal – These records must be shredded.
Child Protection Information held in separate files	Date of Birth of the student plus 25 years then Review ensuring the information has been included on the Local Authority Social Services Record.	
Records of Child Sexual Abuse	Records relating to child sexual abuse (CSA) must be retained for 75 years from the date of birth of the victim. Full records must be preserved, not extracts. Colleagues reviewing	

Student's Educational Record		
File Description	**Retention Period**	**Action at end of Record**
	records will be trained to recognise CSA related material.	
Attendance Records		
Attendance Registers	3 Years after the date on the entry was made	Secure Disposal
Correspondence relating to absence	Current Academic year plus 2 years	
Special Educational Needs ("SEN")		
SEN files, reviews, and individual education plans	Date of Birth of the student plus 25 years	**Review** to suggest there is no potential for litigation against RMAT for "failure to provide a sufficient education." Then Secure Disposal
Education Health Care Plan maintained under section 37 of the Children and Families Act 2014 (and any amendments to the statement or plan)		
Information and advice provided to parents regarding SEND.		
Accessibility strategy		
Student IT Records		
Student IT user ID accounts	Student leaving plus 1 year	Secure Disposal
Student one drives and data stored in colleagues area	Student leaving plus 1 year	
Student Microsoft Office 365 account	Student leaving plus 1 year	

Table 2- Admissions

Admissions		
File Description	**Retention Period**	**Action at end of Record**
Records relating to the creation and implementation of the Academy's Admission Policy.	Life of the Policy plus 3 years then review	Secure Disposal
Admission if the admission is successful.	Date of admission plus 1 year	
Admission – If the appeal is unsuccessful.	Resolution of case plus 1 year	
Register of admissions	3 years after the date of entry	**Review** The Academy may wish to retain permanently to deal with requests from former students
Casual admissions	Current year plus 1 year	Secure Disposal

Admissions		
File Description	**Retention Period**	**Action at end of Record**
Proof of address supplied by parents as part of admissions process		
Supplementary information form including any religious or medical conditions:		
• Successful admissions	Add to student file.	Secure Disposal
• Unsuccessful admissions	Until appeals process is completed.	

Table 3- Student Personal Identifiers

Personal Identifiers, Contact details and personal characteristics		
File Description	**Retention Period**	**Action at end of Record**
Images used for identification purposes.	For the duration of the event/activity or whilst the student remains at the Academy, whichever is shorter, plus one month.	Secure Disposal
Images used in displays.	Whilst the student is at the Academy.	
Images used for marketing purposes.	In line with consent period.	
Biometric data	For the duration of the event/activity or whilst the student remains at the Academy, whichever is shorter, plus one month.	
Postcode, names, and characteristics	Whilst the student is at the Academy plus 5 years	
Address	For the duration of the event/activity plus one month.	

Table 4- Medical Information and administration

Medical Information and administration		
File Description	**Retention Period**	**Action at end of Record**
Permission slips	Duration of administration of medication plus one month	Secure Disposal
Medical conditions-Ongoing management	Included on student file and transferred if student moves on. Copies held whilst the student is at the Academy plus 1 year.	Secure Disposal

Medical Information and administration		
File Description	**Retention Period**	**Action at end of Record**
Medical incidents that have a behavioural or safeguarding influence	Included on student file and transferred if student moves on. Copies held whilst the student is at the Academy plus **25 years**.	

Table 5- Curriculum Management

Curriculum Management		
File Description	**Retention Period**	**Action at end of Record**
Examination papers	Until the appeal/validation process has been completed.	Secure Disposal
Pupil Admission Number ("PAN") Reports	Current academic year plus 6 years.	
Value-added and contextual data		
Self-evaluation forms		

Table 6- Implementation of Curriculum

Curriculum Management		
File Description	**Retention Period**	**Action at end of Record**
Schemes of Work	Current year plus 1 year	Review and allocate a further retention period or Secure Disposal
Timetable		
Class record books		
Mark books		
Record of Homework set		
Students' work	Where possible, work should be returned to students at the end of the academic year. If it is not current year plus 1 year	Secure Disposal

Table 7- Extra-Curricular Activities

Extra-Curricular Activities		
File Description	**Retention Period**	**Action at end of Record**
Records created by an Academy to obtain approval to run an educational visit outside of the classroom	Date of visit plus 10 years	Secure Disposal
Field File	Conclusion of the Trip plus 1 month	**Review** If a minor incident has occurred add to appropriate systems otherwise Secure Disposal.
Finance Information relating to trips	Whilst student remains at Academy plus 1 year	Secure Disposal

Extra-Curricular Activities		
File Description	**Retention Period**	**Action at end of Record**
Parental consent forms	Until the conclusion of the trip	**Review** If a major incident has occurred add to appropriate systems otherwise Secure Disposal.
Records relating to residential trips	Date of birth of youngest student involved plus 25 years	Secure Disposal
Educational visitors to the Academy	Until the conclusion of the visit plus 1 month	

Table 8 - Catering and free school meals

Catering and free school meals		
File Description	**Retention Period**	**Action at end of Record**
Meal Administration	Whilst the student is at the Academy plus 1 year.	Secure Disposal
Meal eligibility	Whilst the student is at the Academy plus 5 years.	

Table 9- Health & Safety

Health & Safety		
File Description	**Retention Period**	**Action at end of Record**
Health & Safety Policy statements	Life of policy plus 3 years.	Secure Disposal
Health & Safety Risk Assessments	Life of risk assessment plus 3 years.	
Records relating to accident/injury at work	Date of incident plus 12 years	**Review** In the case of serious incidents, a further retention period should be applied otherwise Secure Disposal.
Accident Book	Retained for 3 years after last entry. The book may either be on paper or electronic.	**Review** If an incident has been recorded refer to the below otherwise Secure Disposal.
Incident reporting form involving an Adult.	Date of incident plus 25 years.	Secure Disposal
Incident reporting form involving a child.	Date of birth of child plus 25 years.	
Control of Substances hazardous to health (COSHH)	Current year plus 10 years	**Review** Unless serious incident then securely disposes.
Records relating to monitoring of areas where people have encounter Asbestos in an Academy.	Last action plus 40 years.	Secure Disposal
Records relating to monitoring of areas where people have encounter Radiation in an Academy.	Last action plus 50 years	Secure Disposal

Health & Safety		
File Description	**Retention Period**	**Action at end of Record**
Fire precaution logs	Current year plus 6 years	
Fire Risk Assessments	Life of the Risk Assessment plus 6 years.	

Colleague records and other Human Resources related information

123. Retention of all records relating to HR should take into account the recommendations of the Independent Inquiry into Child Sexual Abuse (IICSA). The report from the Inquiry recommended that records associated with child sexual abuse (CSA) should be preserved for 75 years. The Inquiry emphasised the need for this extended retention period due to the significant value these records hold for victims, and advised that they should be subject to regular reviews throughout this duration.

124. In instances where there is evidence or allegations of CSA, schools and academies may decide to retain the complete record, whether of a student, colleague, or other related documents - not merely the segments directly related to the abuse.

125. The Inquiry report advised that the UK government instructs the Information Commissioner's Office (ICO) to develop a Code of Practice concerning the retention of, and access to records known to relate to CSA. This has not been actioned some years following the report's publication, and it is unknown whether this work will be completed. Therefore, there is no statutory requirement to retain these records for such an extensive time period, and a careful management review will need to take place for each record where CSA is relevant before disposal or destruction.

126. In relation to disciplinary and grievance processes, the ACAS Code of Practice recommends that the employee should be told how long a disciplinary warning will remain current. However, this does not mean that the data itself should be destroyed at the end of the set period.

127. Any disciplinary proceedings data will be a record of an important event in the course of the employer's relationship with the employee. Should the same employee be accused of similar misconduct at a later date, reference to the earlier proceedings may be relevant. Alternatively, if the employee were to be dismissed for some later offence and then claim at tribunal that they had e.g. "fifteen years of unblemished service", the record of the disciplinary proceedings would be effective evidence to counter this claim.

128. Employers should, therefore, be careful not to confuse the expiry of a warning for disciplinary purposes with a requirement to destroy all reference to its existence in the personnel file. One danger is that the disciplinary procedure itself often gives the impression that, at the end of the effective period for the warning, the warning will be "removed from the file". This or similar wording should make it clear that, while the warning will not remain active in relation to future disciplinary matters, a record of what has occurred will be kept. Careful attention should be paid to the requirements of the statutory guidance in Keeping Children Safe in Education in relation to any records of disciplinary matters, including inclusion in a reference for a future employer.

129. The Tables below outlines RMAT's retention period for employee records and the action that should be taken after the retention period in line with any requirements. Electronic copies of information and files should also be destroyed in line with the retention period below:

Table 10- Recruitment

Recruitment		
File Description	**Retention Period**	**Action at end of Record**
All records relating to the appointment of the Chief Executive and Academy Principals.	Date of appointment plus 6 years.	Secure Disposal
Records relating to an unsuccessful candidate for appointment.	Date of appointment of successful candidate plus 6 months.	
Records relating to a successful candidate for appointment	Transfer appropriate information to Personal File. Other information destroyed after 6 months	
DBS Check	Copy DBS certificate to be retained on Colleague Personal file for no longer than 6 months	
Proof of identity collected as part of DBS check	Checked and retained on Colleague Personal file	
Evidence of right to work in the UK	Retained on Colleague Personal file.	
Records relating to employment of overseas teachers	Retained on Colleague Personal file.	
Records relating to TUPE process	Date last colleague transfers or leaves RMAT plus 6 years	

Table 11- Operational Colleague Management

Operational Management		
File Description	**Retention Period**	**Action at end of Record**
Colleague Personal File including contract of employment and colleague training records	Termination of employment plus 6 years	Secure Disposal
Timesheets	Current year plus 6 years	
Annual appraisal/assessment records	Current year plus 5 years	
Annual leave records	6 years from the date on which they were made	

Pay and conditions records	Date pays and conditions superseded plus 6 years	
Training needs analysis	Current year plus 1 year	
Colleague IT user ID accounts	Termination of employment plus 3 years	
Colleague one drives and data stored in colleague area	Termination of employment plus 1 year	
Colleague Microsoft Office 365 account	Termination of employment plus 3 years	

Table 12 – Disciplinary and Grievance Processes

Disciplinary and Grievance Processes		
File Description	**Retention Period**	**Action at end of Record**
Child Protection allegation against a colleague including unfounded allegations.	10 years from the date of the allegation.	**Review** to see if any active investigations, then securely dispose. These records must be shredded. *
Disciplinary Proceedings which culminate in:		
• Oral warning	Date of warning plus 6 months	Secure Disposal*
• Level 1 written warning		
• Level 2 written warning	Date of warning plus 12 months	
• Final warning	Date of warning plus 18 months	
Case not found	Conclusion of the case	Secure Disposal unless child protection related*

*If warnings are placed on the personal file, they **must** be weeded from the file at the end of the Retention Period.

Senior Leadership Records

130. The Table below outlines RMAT's retention period for Senior Leadership records and the action that should be taken after the retention period in line with any requirements. Electronic copies of information and files should also be destroyed in line with the retention period below:

Table 13- Senior Leadership Records

Senior Leadership Records		
File Description	**Retention Period**	**Action at end of Record**
Logbooks	Date of last entry in the book plus 6 years then Review.	Offer to Local Records office
Minutes of senior leadership meetings and other regular administrative meetings	Date of the meeting plus 3 years then Review	

Senior Leadership Records		
File Description	**Retention Period**	**Action at end of Record**
Senior Leadership Reports	Date of the meeting plus 3 years then Review	Secure Disposal
Senior Leadership Correspondence	Date of correspondence plus 3 years then Review	
Professional Development Plans	Life of the plan plus 6 years	
Management of Complaints	Date complaint resolved plus 3 years	
Records relating to the management of contracts with external providers	Date of last payment plus 6 years	
Records relating to the management of software licences.	Date licence expires plus 6 years.	
General files	Current year plus 5 years then Review	
Records relating to the creation and publication of an Academy brochure or prospectus	Current year plus 3 years	Disposal
Records relating to student, parent, colleague circulars	Current year plus 1 year	
Newsletters		
Visitor books and signing in records	Current year plus 6 years then Review.	Secure Disposal
Records relating to Parent Teacher/Friends/Former students associations		

Table 14- Statistics and Management Information

Statistics and Management Information		
File Description	**Retention Period**	**Action at end of Record**
Curriculum returns	Current year plus 3 years	Secure Disposal
Examination results (Academy copy)	Current year plus 6 years	
SAT's records:		
• Results	Recorded on student file and retained in accordance with student file. If a composite record is kept, its retention period is current year plus 6 years	

Statistics and Management Information		
File Description	**Retention Period**	**Action at end of Record**
• Examination Papers	Kept until appeals/validation process is complete	Secure Disposal
Published Admission Number repots	Current year plus 6 years	
Value added and contextual data		
Self-evaluation forms		

Finance Records

131. The Tables below outlines RMAT's retention period for Finance records and the action that should be taken after the retention period in line with any requirements. Electronic copies of information and files should also be destroyed in line with the retention period below:

Table 15- Strategic Finance

Strategic Finance		
File Description	**Retention Period**	**Action at end of Record**
Statement of financial activities	Current financial year plus 6 years	Secure Disposal
Financial planning		
Value for money statement		
Records relating to the management of VAT		
Whole of Government accounts returns		
Borrowing Powers		
Budget plan		
Charging and remissions policy	Date policy superseded plus 3 years	

Table 16- Audit Arrangements

Audit Arrangements		
File Description	**Retention Period**	**Action at end of Record**
Audit Committee and Responsible Officers	Life of RMAT	Secure Disposal
Independent Auditors Report on regularity	Financial Year report plus 6 years	
Independent Auditors Report on financial statements		

Table 17- Fuding Agreements

Funding Agreements		
File Description	**Retention Period**	**Action at end of Record**
Funding Agreement with Secretary of State and supplemental funding agreements.	Date of last payment of funding plus 6 years	Secure Disposal
Termination of funding agreement[1]		
Funding Records – Capital Grant		
Funding Records – Earmarked Annual Grant		
Funding Records – General Annual Grant		
Exclusion Agreements[2]	Date of last payment of funding plus 6 years	Secure Disposal
Funding Records[3]		
Gift Aid and Tax Relief		
Records relating to loans	Date of last payment on loan plus 6 years if the loan is under £10,000 or date of last payment on loan plus 12 years if the loan is over £10,000	

Table 18- Payroll and Pensions

Payroll and Pensions		
File Description	**Retention Period**	**Action at end of Record**
Maternity pays records	Current year plus 3 years	Secure Disposal
Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	From the end of the year in which the accounts were signed for a minimum of 6 years	
Management of the Teachers' Pension Scheme	Date of last payment on the pension plus 6 years	
Records relating to pension registrations		
Payroll records	Date payroll run plus 6 years	

[1] Either party may give not less than 7 financial years written notice to terminate the Agreement, such notice to expire on 31 August. Or, where the Academy has significant financial issues or is insolvent, the Agreement can be terminated by the Secretary of State to take effect on the date of the notice.
[2] RMAT can enter an arrangement with a Local Authority, so that payment will flow between RMAT and the LA, in the same way as it would if one of RMAT Academies was a maintained school.
[3] RMAT can only receive donations and charge where the law allows. See charging and remissions policy.

Table 19- Risk Management and Insurance

Risk Management and Insurance		
File Description	**Retention Period**	**Action at end of Record**
Insurance Policies	Date the policy expires plus 6 years	Secure Disposal
Records relating to the settlement of insurance claims	Date Claim settled plus 6 years	
Employer's Liability Insurance Certificate	Closure of the establishment plus 40 years	

Table 20- Endowment Funds and Investments

Endowment Funds and Investments		
File Description	**Retention Period**	**Action at end of Record**
Investment Policies	Life of the Investment plus 6 years	Secure Disposal
Management of Endowment Funds	Life of the fund plus 6 years	

Table 21- Accounts and Statements

Accounts and Statements		
File Description	**Retention Period**	**Action at end of Record**
Annual Accounts	Current year plus 6 years	Standard Disposal
Loans and grants managed by RMAT	Date of last payment of the loan plus 12 years then REVIEW	Secure Disposal
Student Grant applications	Current year plus 3 years	
All records relating to the creation and management of budgets including the Annual budget statement and background papers	Life of the budget plus 3 years	
Invoices, receipts, order books and requisitions, delivery notices	Current financial year plus 6 years	
Records relating to the collection and banking of monies		
Records relating to the identification and collection of debt		

Table 22- Contract Management

Endowment Funds and Investments		
File Description	**Retention Period**	**Action at end of Record**
All records relating to contracts under seal	Last payment on the contract plus 12 years	Secure Disposal
All records relating to contracts under signature	Last payment on the contract plus 6 years	
Records relating to the monitoring of contracts	End of the contract	

Table 23- Asset Management

Asset Management		
File Description	**Retention Period**	**Action at end of Record**
Inventories of furniture and equipment	Current year plus 6 years	Secure Disposal
Burglary, theft, and vandalism reporting forms		
Records relating to the leasing of shared facilities such as sports centres	Current year plus 6 years	
Land and buildings valuations	Date valuation superseded plus 6 years	
Disposal of assets	Date asset disposed of plus 6 years	
Community School leases for land	Date lease expires plus 6 years	
Commercial transfer arrangements	Date of transfer plus 6 years	
Transfer of land to RMAT	Life of land ownership then transfer to new owner.	
Transfers of freehold land		

Table 24- Finance (Banking) Records

Finance and Banking Records		
File Description	**Retention Period**	**Action at end of Record**
Cheque Books	Current Year plus 6 years	Secure Disposal
Paying in Books		
Ledgers		
Invoices		
Receipts		
Bank Statements		

Table 25- School Meals

School Meals[4]		
File Description	**Retention Period**	**Action at end of Record**
Free school meals register	Current year plus 6 years	Secure Disposal
School meals registers	Current year plus 3 years	
School meals summary sheets		

Property Management

132. The Tables below outlines RMAT's retention period for Property Management records and the action that should be taken after the retention period in line with any requirements. Electronic copies of information and files should also be destroyed in line with the retention period below:

Table 26- Property Management

Endowment Funds and Investments		
File Description	**Retention Period**	**Action at end of Record**
Title deeds of properties belonging to RMAT	These should follow the property unless the property has been registered with the Land Registry.	**Review** and discuss with RMAT Company Secretary
Plans of property belonging to RMAT	These should be retained whilst the building belongs to the Academy and should be passed onto any new owners if the building is leased or sold.	
Leases of property leased by or to RMAT	Expiry of lease plus 6 years	Secure Disposal
Records relating to the letting of Academy premises	Current financial year plus 6 years	
Business continuity and disaster recovery plans	Date the plan superseded plus 3 years	

Table 27- Maintenance Records

Maintenance Records		
File Description	**Retention Period**	**Action at end of Record**
All records relating to the maintenance of an Academy conducted by contractors	Current year plus 6 years	Secure Disposal
All records relating to the maintenance of an Academy conducted by Trust		

[4] Unless it would be unreasonable to do so, school lunches should be provided when they are requested by, or on behalf of any student. A school lunch must be provided free of charge to any student entitled to free school meals.

Maintenance Records		
File Description	**Retention Period**	**Action at end of Record**
employees, including maintenance logbooks		

Table 28- Fleet Management

Endowment Funds and Investments		
File Description	**Retention Period**	**Action at end of Record**
Acquisition and disposal of vehicles through lease or purchase, e.g., contracts/leases, quotes, approvals	Disposal of the vehicle plus 6 years	Secure Disposal
Allocation and maintenance of vehicles, e.g., who drives the vehicle and when and maintenance logs		
Service logs and vehicle logs	Life of the vehicle plus 6 years or if a lease vehicle returned to the leasing company	
GPS tracking data relating to the vehicles	Date of journey plus 6 years	

Governance Records

133. The Tables below outlines RMAT's retention period for Governance records and the action that should be taken after the retention period in line with any requirements. Electronic copies of information and files should also be destroyed in line with the retention period below:

Table 29- Main Governance Documents

Governance of RMAT		
File Description	**Retention Period**	**Action at end of Record**
Governance Statement	Life of Governance statement plus 6 years	Secure Disposal
Articles of Association	Life of RMAT	**Review** and then disposal
Memorandum of Association	Disposal following incorporation	Secure Disposal
Memorandum of Understanding of Shared Governance among Schools	Life of Memorandum of Understanding plus 6 years	Secure Disposal
Constitution	Life of RMAT	**Review** and then disposal
Special Resolutions to amend the Constitution		
Written Scheme of Delegation	Life of Written Scheme of Delegation plus 10 years	
Appointment of Trustees	Appointment plus 6 years	

Governance of RMAT		
File Description	**Retention Period**	**Action at end of Record**
Disqualification of Trustees	Date of Disqualification plus 15 years	Secure Disposal
Termination of Trustee Office	Date of Termination plus 6 years	
Annual Trustee's Report	Date of report plus 10 years	
Annual Report and Accounts		
Annual Return		
Appointment of Trustees and Local Review Board ("LRB") Members	Life of appointment plus 6 years	
Statement of Trustees Responsibilities		
Appointment and Removal of Members		
Strategic Review	Life of the review/plan or until review/plan superseded + 3 years. If major changes are made to the review, then an archive copy of previous review/plan should be retained	
Strategic Plan		
Accessibility Plan		
Academy Restrictive Intervention Record	6 years or longer where injury or SEND is involved	Review then Secure Disposal

Table 30-Trust Governance Minutes

Governance of RMAT		
Trustees		
File Description	**Retention Period**	**Action at end of Record**
Trust Board Meeting Minutes	Minimum of 10 years from the meeting	**Review** and Offer to Archives[5]
Trust Board Decisions		
Governance Planner	Current Year	Secure Disposal
Procedures for conduct at Board meetings	Date procedures superseded plus 6 years	
Committee meeting Minutes[6]	Minimum of 10 years from the meeting	**Review** and Offer to Archives
Members		
File Description	**Retention Period**	**Action at end of Record**

[5] RMAT will identify records of permanent historical value and consider transferring them to the local records office, including digital archives where applicable. Social media content may form part of the institutional record.

[6] RMAT Board may establish any committee and determine the constitution, membership and proceedings that will apply. These will be included in the Terms of Reference

Governance of RMAT		
Records relating to the management of General Members Meetings[7]	Minimum of 10 years from the meeting	**Review** and Offer to Archives
Records relating to the management of Annual General Meetings[8]		
Local Review Boards ("LRB's")		
Agendas for LRB meetings	Retain 1 copy with the master set of minutes.	Secure Disposal
Minutes of and papers considered at LRB meetings		
Master set of Minutes	Life of the Academy	Disposal
Reports Presented to the LRB	Minimum of 6 years	Secure Disposal or retain with the Master set of Minutes
Records relating to complaints dealt with by the LRB	Date of resolution of the complaint plus a minimum of 6 years then review for further retention in case of contentious disputes	Secure Disposal
Statutory Registers[9]		
Register of Trustees	Life of RMAT + 6 Years	Secure Disposal
Resister of Trustees Interests[10]		
Register of Trustee's residential addresses		
Register of Gifts and Hospitality		
Register of Members		
Register of Secretaries		
Register of Trustees Interests		
Declaration of Interests statements[11]		

Table 31- Local Authority Returns

Local Authority		
File Description	**Retention Period**	**Action at end of Record**
Secondary Transfer Sheets (Primary)	Current Year plus 2 years	Secure Disposal
Attendance Returns	Current Year plus 1 year	
School Census Return	Current Year plus 5 years	

[7] The minutes must be kept securely together with the notice and agenda for the meeting and supporting documentation provided for consideration at the meeting.
[8] Ibid.
[9] Trusts are required by law to keep specific records. The registers record information relating to RMAT's operation.
[10] Not a statutory register
[11] Ibid.

Table 32- Central Government Reports/Returns

Central Government		
File Description	**Retention Period**	**Action at end of Record**
OFSTED reports and papers	Life of the report then **Review**	Secure Disposal
Returns made to central Government	Current year plus 6 years	
Circulars and other information sent from central government	Operational use	

Table 33 - Policies and Frameworks

Policies and Framework		
File Description	**Retention Period**	**Action at end of Record**
Complaints Policy	Life of the policy or policy superseded + 3 years. If major changes are made to the policy, then an archive copy of previous policies should be retained	Secure Disposal
Data Protection Policy		
FOI Policy		
Information Governance & Security Policy		
SEND Policy		
Equality Information and Objectives (Public sector equality duty)		
Risk and Control Framework		

CCTV

134. The Table below outlines RMAT's retention period for CCTV images and the action that should be taken after the retention period in line with any requirements.

Table 34: CCTV images

CCTV Images		
File Description	**Retention Period**	**Action at end of Record**
For crime prevention purposes	Until the end of any criminal proceedings then **Review**	Secure Disposal
Other images	Up to 90 days	

Digital Systems & Electronic Records

135. The Table below outlines RMAT's retention period for Digital Systems & Electronic Records and the action that should be taken after the retention period in line with any requirements.

Table 35- Digital & Electronic Records

Digital Systems & Electronic Records				
File/Data Type	**Retention Period**	**Trigger**	**Action at End of Retention**	**Basis/Notes**
System Metadata	Retain for the life of the associated record. Where metadata is system-generated and not tied to a specific record, retain for system life + 1 year.	End of retention period of relevant record OR decommissioning of system.	Secure deletion or placement beyond use.	Metadata is necessary for authenticity, integrity and usability of digital records.
Cloud Backups (Office 365)	Maximum of 30 days unless longer retention is contractually or operationally required. Backups must never exceed the retention period of the source data.	Date backup created.	Automated secure deletion.	Guidance requires deletion capability and avoidance of vendor lock-in; backups must not extend retention periods beyond lawful necessity.
Microsoft Teams Meeting Recordings	Standard: 30 days. If minutes or formal record required: retain until minutes are approved. If safeguarding-related: transfer to safeguarding system and apply safeguarding retention.	Date of recording	Secure deletion from system.	No set retention. Deletion after producing minutes recommended. Safeguarding exceptions apply

File/Data Type	Retention Period	Trigger	Action at End of Retention	Basis/Notes
Teams Chat History/Channel Posts	6 months unless content is moved to an official record (e.g. student file, HR file, safeguarding).	Date of message.	Secure deletion.	Electronic communication is not a record unless captured into record-keeping systems. Deleted items folders do not constitute deletion.
Email Backups/Email Archives	6 months for standard accounts; 6 months after departure for leavers.	End of period OR employee leaving.	Automatic deletion, ensuring all backup copies removed.	Email should not be used as a filing system; RMAT requires automatic deletion.
Safeguarding Systems Archives	Retain only until confirmation of successful transfer to new school. Thereafter delete unless RMAT academy is last known school, in which case retain to DOB + 25 years.	Student transfer or determination the RMAT academy is last known school.	Secure deletion OR archive retention to DOB + 25 years.	Guidance emphasises accidental retention of archived safeguarding records after transfer, requiring deletion.
Safeguarding Incident Exports	Add to student safeguarding file and apply safeguarding retention (DOB + 25 years; 75 years for CSA).	Date of creation	Secure deletion if duplicate; otherwise retain with safeguarding file.	CSA retention 75 years; safeguarding files 25 years from DOB.
Digital Continuity Copies	Life of record + 1 year	End of retention period	Secure deletion	All records >6 years require digital continuity planning.
MIS Audit logs	1 year unless required for investigation; then retain until matter concludes + 6 months	Date of log		Must support security, FOI and SAR compliance.
System configuration Documentation & Data dictionaries	Life of system + 6 years.	Decommission of system		Required for demonstrating integrity and consistency of stored data.

Cloud System Decommissioning Images/ Data Exports	6 months following verified successful migration.	Date of migration		Supports vendor exit and continuity; must not be retained long-term.

Other Documents

101. This policy should be read in conjunction with the following RMAT Policies:

- Data Protection and Information Governance Policy.
- Information Asset Register.
- IT Security Policy; and
- Freedom of Information Policy and Publication Scheme

Monitoring

102. The COO will monitor the implementation and effectiveness of the policy by monitoring reports made under the policy.

103. The COO will monitor the relevant legislation, guidelines, and information forthcoming from the relevant statutory bodies for any recommendation or changes. Where a gap, potential inequality or shortfall in performance is identified within the policy, the COO will advise the Board of Trustees of any changes that are needed, and a proposal will be submitted to the RMAT Board within an appropriate timescale. There will be a full review of the policy by the COO prior to the stated review date where recommendations will be made for consideration by the RMAT Board.