RECORDS MANAGEMENT POLICY

Summary	Records Management Policy
Responsible Person/Author:	Head of Governance and Compliance
Applies to: (please circle/delete as appropriate)	Staff ☒ Student☒ Community ☐
Ratifying Committee(s)	Trust Board
Available On:	Website, Staff Drives, On Demand
Date of Approval	30.05.2022
Effective from:	01.06.2022
Date of Next Formal Review:	April 2024
Review Period	2 Years
Status:	Non-Statutory
Owner	The Rodillian Multi Academy Trust
Version:	2

Document Control

Date	Version	Action	Amendments
14.05.22	2	Policy updated from policy approved in 2018	Multiple

Contents

Records Management Retention Tables

Introduction

1. The Rodillian Multi Academy Trust ("the Trust") 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 the Trust. Records provide evidence for protecting the legal rights and interests of the Trust and provide evidence for demonstrating performance and accountability.

Scope and Purpose of this Policy and who it applies to.

2. This policy provides for how the Trust will provide the effective management of its records including audit purposes.

3. The policy applies to all records created, received or maintained by permanent and temporary staff of the Trust in the course of carrying out is functions. Also, by any agents, contractors, consultants or third parties acting on behalf of the Trust.

4. Records are defined as all those documents which facilitate the business carried out by the Trust 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, e.g. paper documents, scanned documents, e-mails which document Trust decisions and activities, audio and video recordings, text messages, notes of telephone and other forms of verbal communication conversations, spreadsheets, Microsoft word documents, and presentations.

Publication of this Policy

5. This policy will be available to all staff, 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 the Trust's Data Protection Officer ("DPO"). amarham@rodillianacademy.co.uk.

Responsibility for and under this Policy

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

7. 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.

8. The DPO will undertake 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.

9. The Trust 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.

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

- Manage the Trust'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.

Aims of this Policy

11. To set out how the Trust will manage its Records.

12. To support the values of the Trust and its Academies.

Student Records

13. The Trust 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.

14. Student Records held in the Trust 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. Staff 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"). The Trust treats requests for information from students or parents as requests under Data Protection legislation.

Paper Files

15. 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")

16.   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:

17.   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 staff:

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

Records not forming part of the Student Record

18.   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

19.   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 transfer other than duplicates or records with a shorter retention period which should already have been disposed of.

Transfer Process

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

- SIMS information should be transferred by Common Transfer File 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.

Independent School or a Post 16 Establishment

21.   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

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

Retention of Records Post Transfer

23.   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.

24.   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.

25.   All child protection files should be retained.

Last Known Academy

26.   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.

27.   The student record should be retained as a whole for 25 years from the date of birth of the student after which time it can be deleted or destroyed.

Information Audits

28.   Information Audits allow the Trust to consider:

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

29.   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.

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

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

32. The benefit of Information Audits are as follows:

- The Trust can manage information in order to get the most effective use from it;
- The Trust can more easily manage information taking into account 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 the Trust to demonstrate compliance with the DPA.

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

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

34. 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.

35. 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

36. 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.

37. 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 are easy to copy regardless of your decision to delete it.

E-mail

38.   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.

39.   Confidential or sensitive information should **only** be sent by a secure encrypted e-mail or data transfer system. A student's name or other personal information should never be put in the subject heading.

40.   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.

41.   When considering whether to retain an email and its attachment, staff 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.

42.   The Trust intends that emails should be deleted from a user's inbox after 6 months. Employees who leave the Trust 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 the Trust should have their user inbox immediately deleted.

Faxes

43.   If a Member of staff is sending confidential information by fax, staff should check the recipient is correct before sending the fax.

Microsoft Teams

44.   Staff, 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

45.   If members of staff or 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

46.   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.

47.   Any member of staff who is responsible for a social media account should familiarise themselves with the account's retention period. Before publishing any item on social media,

staff 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.

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

Digital Continuity Statement

49.   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.

50.   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.

51.   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.

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

53.   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.

54.   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

55.   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.

56.   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

57. 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

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

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

60. 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.

61. 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.

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

Taking Records off Trust Premises and Sharing Records

63. 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, staff 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.

64. Before sharing data, staff 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

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

66.   Under no circumstances should visitors be allowed access to confidential or personal information. Visitors to areas where sensitive information is stored should be supervised at all times.

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

68.   Students/Parents or staff who request information held by the Trust 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

69.   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.

70.   Disposal must be carried out 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.

71.   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.

72.   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.

Destruction of Records by Type:

(1)   Paper Records

73.   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.

74.   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.

75.   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.

76.   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

50.   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.

51.   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.

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

53.   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

54.   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.

55.   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.

56.   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

57.   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.

58.   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.

59.   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

60.   **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.

61.   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.

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

Physical Storage of Records:

63.   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.

64.   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%).

65.   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.

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

Retention Periods:

Student records and other student related information

67.   The Tables below outlines the Trust'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 Exclusion Records	Date of Birth of student plus 25 years	Secure Disposal
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	Secure Disposal – These records must be shredded.

Student's Educational Record		
File Description	**Retention Period**	**Action at end of Record**
	sealed envelope on the student file.	
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.	
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** in order to suggest there is no potential for litigation against the Trust 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		

*it is recommended that no child protection files are destroyed until the conclusion of the Independent Inquiry on Historical Child Sex Abuse

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

Admissions		
File Description	**Retention Period**	**Action at end of Record**
		deal with requests from former students
Casual admissions	Current year plus 1 year	Secure Disposal
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	Secure Disposal

Medical Information and administration		
File Description	Retention Period	Action at end of Record
	student is at the Academy plus 1 year.	
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 isn't 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.

Extra-Curricular Activities		
File Description	**Retention Period**	**Action at end of Record**
Finance Information relating to trips	Whilst student remains at Academy plus 1 year	Secure Disposal
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 dispose.
Records relating to monitoring of areas where people have come into contact with Asbestos in an Academy.	Last action plus 40 years.	Secure Disposal
Records relating to monitoring of areas where people have	Last action plus 50 years	Secure Disposal

Health & Safety		
File Description	**Retention Period**	**Action at end of Record**
come into contact with Radiation in an Academy.		
Fire precaution logs	Current year plus 6 years	
Fire Risk Assessments	Life of the Risk Assessment plus 6 years.	

Staff records and other Human Resources related information

68.   The Tables below outlines the Trust'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 Staff Personal file	
Proof of identity collected as part of DBS check	Checked and retained on Staff Personal file	
Evidence of right to work in the UK	Retained on Staff Personal file	
Records relating to employment of overseas teachers		
Records relating to TUPE process	Date last member of staff transfers or leaves the Trust plus 6 years	

Table 11- Operational Staff Management

Operational Management		
File Description	**Retention Period**	**Action at end of Record**
Staff Personal File including contract of employment and staff 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	
Pay and conditions records	Date pay and conditions superseded plus 6 years	
Training needs analysis	Current year plus 1 year	

Table 12 – Disciplinary and Grievance Processes

Disciplinary and Grievance Processes		
File Description	**Retention Period**	**Action at end of Record**
Child Protection allegation against a member of staff 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*

* All records relating to child protection issues including warnings should be retained until the completion of the Independent Inquiry on Child Sexual Abuse. This part of the retention schedule will be reviewed following the final report of the Inquiry.

#If warnings are placed on the personal file they **must** be weeded from the file at the end of the Retention Period subject to the comments above.

Senior Leadership Records

69.   The Table below outlines the Trust'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**
Log Books	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	Secure Disposal
Senior Leadership Reports	Date of the meeting plus 3 years then Review	
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, staff 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	

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

Finance Records

70.   The Tables below outlines the Trust'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 the Trust	Secure Disposal
Independent Auditors Report on regularity	Financial Year report plus 6 years	

Audit Arrangements		
File Description	**Retention Period**	**Action at end of Record**
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 pay 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	

---

[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] The Trust can enter into an arrangement with a Local Authority, so that payment will flow between the Trust and the LA, in the same way as it would if one of the Trust Academies was a maintained school.

[3] The Trust can only receive donations and charge where the law allows. See charging and remissions policy.

Payroll and Pensions		
File Description	**Retention Period**	**Action at end of Record**
Records relating to pension registrations	pension plus 6 years	
Payroll records	Date payroll run plus 6 years	

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 the Trust	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	Current year plus 2 years	

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 the Trust	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	
School meals registers	Current year plus 3 years	Secure Disposal
School meals summary sheets		

Property Management

71. The Tables below outlines the Trust'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 the Trust	These should follow the property unless the property has been registered with the Land Registry.	**Review** and discuss with the Trust Company Secretary
Plans of property belonging to the Trust	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 the Trust	Expiry of lease plus 6 years	
Records relating to the letting of Academy premises	Current financial year plus 6 years	Secure Disposal
Business continuity and disaster recovery plans	Date the plan superseded plus 3 years	

---

[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.

Table 27- Maintenance Records

Maintenance Records		
File Description	**Retention Period**	**Action at end of Record**
All records relating to the maintenance of an Academy carried out by contractors	Current year plus 6 years	Secure Disposal
All records relating to the maintenance of an Academy carried out by Trust employees, including maintenance log books		

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

72. The Tables below outlines the Trust'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 the Trust		
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 the Trust	**Review** and then disposal
Memorandum of Association	Disposal following incorporation	Secure Disposal

Governance of the Trust		
File Description	**Retention Period**	**Action at end of Record**
Memorandum of Understanding of Shared Governance among Schools	Life of Memorandum of Understanding plus 6 years	Secure Disposal
Constitution	Life of the Trust	**Review** and then disposal
Special Resolutions to amend the Constitution		
Written Scheme of Delegation	Life of Written Scheme of Delegation plus 10 years	Secure Disposal
Appointment of Trustees	Appointment plus 6 years	
Disqualification of Trustees	Date of Disqualification plus 15 years	
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	Date of Review plus 6 years	
Strategic Plan	Life of plan plus 6 years	
Accessibility Plan		

Table 30-Trust Governance Minutes

Governance of the Trust		
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
Trust Board Decisions		
Governance Planner	Current Year	Secure Disposal
Procedures for conduct at Board meetings	Date procedures superseded plus 6 years	
Committee meeting Minutes[5]	Minimum of 10 years from the meeting	**Review** and Offer to Archives

---

[5] The Trust 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 the Trust		
Members		
File Description	**Retention Period**	**Action at end of Record**
Records relating to the management of General Members Meetings[6]	Minimum of 10 years from the meeting	**Review** and Offer to Archives
Records relating to the management of Annual General Meetings[7]		
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[8]		
Register of Trustees	Life of the Trust + 6 Years	Secure Disposal
Resister of Trustees Interests[9]		
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[10]		

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	

---

[6] The minutes must be kept securely together with the notice and agenda for the meeting and supporting documentation provided for consideration at the meeting.

[7] Ibid.

[8] Trusts are required by law to keep specific records. The registers record information relating to the Trust's operation

[9] Not a statutory register

[10] Ibid.

Table 32- Central Government Reports/Returns

Local Authority		
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	

Other Documents

77.   This policy should be read in conjunction with the following Trust Policies:

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

Monitoring

78.   The Head of Governance and Compliance will monitor the implementation and effectiveness of the policy by monitoring reports made under the policy.

79.   The Head of Governance and Compliance 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 Head of Governance and Compliance will advise the Board of Trustees of any changes that are needed and a proposal will be submitted to the Trust Board within an appropriate timescale. There will be a full review of the policy by the Head of Governance and Compliance prior to the stated review date where recommendations will be made for consideration by the Trust Board.

Diversity

80.   The Rodillian Multi Academy Trust is committed to a policy of celebrating diversity, promoting equality of opportunity, providing an inclusive workplace, and eliminating any unfair treatment or unlawful discrimination. This overriding objective applies to all policies and procedures relating to staff and students. The Trust will always comply with the requirements of the Equality Act 2010 and associated guidance produced by the Department for Education.

Appendix 1: Equality Impact Assessment

Equality, Diversity, Cohesion, and Integration Screening.

As a public authority, the Rodillian Multi Academy Trust needs to ensure that all our strategies, policies, service, and functions, both current and proposed have had proper consideration of equality, diversity, cohesion, and integration.

A **screening** process can help judge relevance and provides a record of both the **process** and **decision.** Screening should be a short, sharp exercise that determines relevance for all new and revised strategies, policies, services, and functions. Completed at the earliest opportunity it will help to determine:

- the relevance of proposals and decisions to equality, diversity, cohesion, and integration.
- whether or not equality, diversity, cohesion, and integration is being/has already been considered, and
- whether or not it is necessary to carry out an impact assessment.

Organisation: The Rodillian Multi- Academy Trust	Department responsible for the Policy: Head of Governance and Compliance
Lead Person: Adam Marham	**Contact Number:**

1. Title: Freedom of Information Policy and Publication Scheme

2. Please provide a brief description of what you are screening
The Policy

3. Relevance to equality, diversity, cohesion, and integration

Questions	Yes	No
Is there an existing or likely differential impact for the different equality characteristics?		x
Have there been or likely to be any public concerns about the Policy or proposal?		x
Could the proposal affect how services are organised, provided, located and by whom?	x	
Could the proposal affect our workforce or employment practices?	x	
Does the proposal involve or will it have an impact on: -?		
• Eliminating unlawful discrimination, victimisation, and harassment		X
• Advancing equality of opportunity		X
• Fostering good relations	x	

4. Considering the impact on equality, diversity, cohesion, and integration
• **Scope of the proposal:** Students, parents, staff, the community.
• **Who is likely to be affected?** Students, parents, staff, the community.
• **Consultation and engagement activities with those likely to be affected?** Ongoing feedback from Students, parents, staff, the community. The Policy is available through the Trust and Academies websites and a written copy can be provided on request.
• **Key findings**
We have considered the potential positive and negative impact on different equality characteristics in relation to the Policy and do not believe that any groups will be adversely affected. The Trust is vigilant in adhering to the appropriate legislation in relation to protected characteristics and to preventing discrimination. Managers are supported and trained in relation to these areas. The Policy has considered religious, racial and gender-specific clothing requirements and those of staff with disabilities in line with the Equality Act. We have considered the perception that the proposal could benefit one group at the expense of another and we do not believe that the Policy could be perceived to be discriminatory with regards to its wording or format.
• **Actions**
The Trust will continue to promote positive impact and remove/reduce negative impact through the application of this Policy within the organisation.

5. Governance, ownership, and approval		
Please state here who has approved the actions and outcomes of the screening		
Name	**Job title**	**Date**
Adam Marham	Head of Governance and Compliance	14.05.22

6. Publishing	
This screening document will act as evidence that due regard to equality and diversity has been given.	
Date screening completed	14.05.22
Date agreed at Trust Board	30.05.22