

Salendine Nook High School (Academy)

Records, Retention and Disposal Policy

**(Non-Statutory)
Recommended practice – DfE & DPO**

Date policy written:	September 2022
Produced by:	Mrs V Wood
Approved by SLT:	28.9.22
Review date:	September 2024

Statement for Salendine Nook Academy Trust

TABLE OF CONTENTS

1. INTRODUCTION
2. PURPOSE OF THIS POLICY
3. SCOPE OF THIS POLICY
4. DEFINITIONS
5. AIMS OF THE POLICY
6. STATEMENT OF POLICY RETENTION OF RECORDS
7. DISPOSAL OF RECORDS
8. REVIEW OF RECORDS
9. DUPLICATE RECORDS
10. ROLES AND RESPONSIBILITIES
11. TRAINING AND AWARENESS
12. POLICY COMPLIANCE AND AUDIT
13. POLICY GOVERNANCE
14. COMPLAINTS
15. REVIEW AND MAINTENANCE
16. ENQUIRIES
17. SUPPORTING POLICIES/DOCUMENTS
DOCUMENT HISTORY AND VERSION CONTROL
REVIEW AND APPROVAL
APPENDIX A
APPENDIX B
APPENDIX C

1. INTRODUCTION

- 1.1 This policy applies to Salendine Nook Academy Trust (hereafter referred to as the Academy) which is a registered company, limited by guarantee, in England and Wales under registration number 07883174, with a registered office at Salendine Nook High School Academy, New Hey Road, Huddersfield, West Yorkshire, HD3 4GN.
- 1.2 The Data Protection Act (DPA) 2018 and the UK General Data Protection Regulations (UK GDPR) provide the law which safeguards personal privacy, giving protection to individuals as to how their personal information is used. It applies to anyone who handles or has access to people's personal data.
- 1.3 Schools are required to have a retention policy which must comply with the UK GDPR. This is because every school is classed as a Data Controller under the data protection legislation because they decide how personal data for which they are responsible is processed and disposed of.
- 1.4 The Department for Education (DfE) recommended guidance on this is the Information Management Toolkit for Schools (IMRS), which is sponsored by Tribal. This toolkit can be used as a supporting document in addition to this policy. A more detailed specific list relating to financial procedures is detailed in the Academy's Financial Procedures Manual. This manual is compliant with the IMRS Toolkit.
- 1.5 The Information Commissioner as the Regulator can impose fines of up to £17.5 million for serious breaches of the UK GDPR, and other fines/disciplinary action for other breaches of data protection legislation, therefore it is imperative that the Academy and all staff comply with the legislation.
- 1.6 The Academy collects and uses a large amount of personal information every year about staff, pupils, parents, carers, and other individuals who come into contact with the school in order to operate. By way of example, this includes pupil records, staff records, names, and addresses of those requesting prospectuses, test marks, references, and fee collection from Local Authorities (LAs), government agencies and other bodies. In addition, there may be a legal requirement for the Academy to process personal information to ensure that it complies with statutory obligations.
- 1.7 Any failure to comply with any part of this policy may lead to disciplinary action under the Academy's procedures and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

2. PURPOSE OF THIS POLICY

- 2.1 This policy is a part of a set of Information Governance policies and procedures that support the delivery of the Information Governance Framework. It should be read in conjunction with these associated policies. The purpose of this policy is to set out how the Academy handles personal data.
- 2.2 Physical or electronic documents and records may need to be retained in order to fulfil statutory or regulatory requirements, to evidence events/agreements in the case of dispute(s) or meet operational needs.
- 2.3 However, keeping records that are not required is unlawful.
- 2.4 The untimely destruction of documents to which one or more of the criteria in paragraph 2.2 is applicable, could cause the Academy difficulty in defending a claim or prosecution brought against it or could cause operational problems or embarrassment to the organisation. Conversely, retaining records for too long could result in a breach of the UK General Data Protection Regulations and Data Protection Act 2018. The permanent retention of all documents and records is undesirable, uneconomical, and unsustainable.
- 2.5 This policy, therefore, outlines the need for records to be retained for agreed periods of time, reviewed if necessary, and disposed of according to rules which will be clearly stated on retention schedule documents.
- 2.6 Failure to adhere to this policy could result in fines and penalties, along with damage to reputation.

3. SCOPE OF THIS POLICY

- 3.1 This policy applies to everyone who has access to the Academy's information, information assets or IT equipment. These people are referred to 'users' in this policy. This may include but is not limited to employees, temporary workers, partners and contractual third parties.
- 3.2 This policy is relevant to records of the Academy. A 'record' is defined as follows:
- Information that is **created or received, captured, and maintained as evidence** of the business of Academy, due to its operational, legal, or financial value to the organisation.
- 3.3 This policy covers records in all physical and electronic formats; including, but not restricted to:
- Paper;
 - Electronic documents;

- Emails;
- Voicemail;
- Web records such as blogs, wikis, and discussion threads;
- Other records created in social media used for business purposes, such as Twitter;
- Visual images such as photographs;
- Scanned images;
- Microform, including microfiches & microfilm;
- Records stored on removable media, such as audio and video tapes, memory sticks, CDs, DVDs, and cassettes;
- Published web content (Intranet/Internet/Extranet); and
- Databases and spreadsheets.

This policy will also cover formats that are developed and used in the future.

3.4 This policy does not cover documents that are not Academy, for example, non-work-related emails, stationery, or reference material.

3.5 This policy applies to all of the Academy's personal data processing functions, including those performed on customers', clients', employees', suppliers' and partners' personal data, and any other personal data the organisation processes from any source.

3.6 This policy is applicable to all personal data held by the Academy whether the information is held or accessed on company premises, on removable devices and other portable media, or accessed via mobile or home working.

3.7 Endorsement of this policy is mandatory at induction and should be refreshed through training annually.

4. DEFINITIONS

4.1 See 'Appendix B Glossary'

5. AIMS OF THE POLICY

5.1 To promote the development and approval of a retention and disposal schedule which will enable improved and consistent record retention and disposal practices across the Academy;

5.2 To ensure that Academy only retains records that are required by law or to support the activities or transactions of the organisation;

- 5.3 To outline the standards that must be met to ensure appropriate retention and disposal of Academy records;
- 5.4 To ensure that the Academy complies with relevant regulations and legislation, for example, the General Data Protection Regulation and Data Protection Act 2018;
- 5.5 To protect Academy against the risks associated with retaining records for too long, or disposing of them too soon;
- 5.6 To promote the identification of records which require permanent preservation to ensure the protection of the Academy's memory;
- 5.7 To ease pressures on physical and electronic storage space, facilitate fast retrieval of records, and improve staff confidence in records, by reducing the volume of records that are kept unnecessarily.
- 5.8 To ensure that when additional information governance rules (for example security classifications) are applied to records, this is carried out in the most efficient way possible, as these rules will only be applied to records that actually need to be retained.

6. STATEMENT OF POLICY RETENTION OF RECORDS

- 6.1 It is a requirement of this policy that all Academy records are retained and disposed of in accordance with clear rules agreed upon between relevant School functions, Record Managers, and taking into account legal or regulatory requirements. Rules stating how long records will be kept for (retention periods), and the manner of disposal at the end of these retention periods, will be outlined in the Academy's retention and disposal schedule, which will be subject to an annual review. Retention periods should be assigned to existing records retrospectively (as far as possible) and to all newly created records.
- 6.2 The length of the retention period will depend on the type of record and its value to Academy, and any legislation or standards that might apply. Where possible, disposal, review or transfer dates will be recorded on, or within the record or collection of records.
- 6.3 Most records will need to be kept for a reasonable period of between six months and six years, however, they may be retained for longer periods when:
- The information contained in them is relevant to a legal action which has been started or is pending. If such action is pending, a note should be appended to any physical file stating that the records should not be destroyed. Electronic records should be flagged to prevent erasure;

- There is a legal/organisational necessity to keep specific records for longer than the six-year period;
- They are required to be kept longer by statute. A number of Acts, for example, the Latent Damage Act (1986), and regulations govern the retention of certain types of records;
- They consist of information maintained for the purpose of retrospective comparison. For example, tracking service improvement or service profiling data;
- They are required for the purpose of staff disciplinary proceedings; or
- They relate to contracts ‘under seal’ between Academy and a third party.

6.4 The Academy’s retention schedule will be created within a standard template, an example of which can be found in Appendix A.

6.5 Where records contain personal information, the fifth principle of the GDPR must be satisfied – ‘personal data should not be kept for longer than necessary’.

6.6 As far as possible, similar records across the organisation will be held for the same length of time. The Academy information governance (IG) team will have an overarching role in the development of the Academy retention schedule, to ensure this consistency is achieved.

6.7 The Academy’s retention schedule will take account of any existing schedules during development, and will supersede these once it has been approved, in order to achieve consistency as outlined in 5.8. As an example, the retention rules for key financial documents are currently set out within an appendix to the existing Financial Procedure Rules, which will be removed once the Academy’s retention schedule is in place.

6.8 Documents that are not Academy records, as per the examples in 3.3, should be disposed of once their usefulness has passed.

7. DISPOSAL OF RECORDS

7.1 Records must be disposed of appropriately once their retention period has expired. Records should not be retained beyond disposal dates, and therefore services must consider the practicality of disposing of records in accordance with the relevant date.

7.2 Physical and electronic records must be disposed of appropriately in line with the ‘guidance on the disposal of records’, available here. It should be noted that school staff are instructed to delete e-mails at the end of each academic year.

7.3 Retention rules must cover 'archived' data and data held on backup tapes, to ensure clarity over when a record has actually been deleted. The IT Department are responsible for the destruction of data held on backup tapes in line with the retention schedule.

7.4 Where records are destroyed a record must be kept, containing all the information outlined in the template in Appendix B. Disposal records should demonstrate that the disposal was in accordance with this policy, or a written record should be made justifying the reasons for departure from this policy. If records are destroyed by external organisations on behalf of the Academy, a certificate of destruction should be provided to and held by, the relevant Records Manager.

7.5 If a record due for destruction is known to be the subject of a request for information under the Data Protection Act 2018 or Freedom of Information Act (2000), destruction should be delayed until disclosure has taken place or, Academy has decided not to disclose the information, until the complaint or appeal provisions of the relevant legislation have been exhausted.

8. REVIEW OF RECORDS

8.1 When a review date is reached, a review should be undertaken to determine if the record can be disposed of, or if a further review or disposal date needs to be assigned. Where records are not destroyed as a result of the review, this action, and the reasons for it, must be clearly justified, and documented within the disposal record.

9. DUPLICATE RECORDS

9.1 Many records will exist in both electronic and physical formats, and multiple copies may exist. The creation of duplicate records should be kept to a minimum, for example when copies of meeting papers are printed, these copies should be disposed of as soon as they are no longer needed for reference. If duplication is necessary, then a decision must be taken as to which copy is the 'master' copy record, and retention rules should reflect this decision. If one copy is destroyed but others still exist, then Academy still holds the information, and this could increase the risk of a breach of the GDPR or Data Protection Act 2018.

9.2 Where the decision is taken that an electronic copy is the 'master' copy of a record, then consideration must be given to any potential legal admissibility issues that may arise. For further information please contact the Academy's information governance team.

10. ROLES AND RESPONSIBILITIES

10.1 Any records created by employees of Academy or transferred to Academy by an external organisation, become an Academy asset, and are the property of Academy.

10.2 **Individual employees** are responsible for ensuring that:

- the policy and any related procedures are adhered to;
- all records, regardless of format, are managed in line with Academy policy; and
- the Academy retention schedule, once approved, is adhered to, and consequently, records are disposed of or reviewed as necessary;
- e-mail is primarily a communications tool, and e-mail applications are not designed for keeping e-mail as a record in a storage area meeting records management storage standards. However, it may be that some e-mails do need to be kept and should therefore be identified by content; for example, if it forms part of a pupil record or a staff /supplier contract. The retention for keeping these e-mails will then correspond with the classes of records according to the content in the retention schedule for schools found in the Records Management Tool Kit for Schools.

These e-mails may need to be saved into any appropriate electronic filing system or printed out and placed on paper files.

If an e-mail is not required to be kept then staff should delete these e-mails within a reasonable timeframe, which would be a maximum of 12 months.

The end of each academic year would be a good time for staff to complete a housekeeping exercise on their kept e-mails, but this may also be done throughout the school year.

10.3 The **Governing Body** has ultimate responsibility for the Records Retention and Disposal Policy within the Academy. Implementation of and compliance with this policy is delegated to the designated Data Protection Manager (**Director of Finance & Resources**) in consultation with the Data Protection Officer (DPO), where necessary.

10.4 The **Director of Finance & Resources** will be responsible for:

- ensuring that users are fully informed of their obligations and responsibilities with respect to information governance policies, standards, guidelines, and procedures;
- ensuring that breaches of information governance policies are brought to the attention of the appropriate employee assigned responsibility for information governance, at the earliest opportunity; and

- ensuring that temporary staff or external contractors only access information required to perform their duties and are provided information security training before handling any information.

10.5 **Senior Leadership Team (SLT)** will be responsible for developing, advising, and monitoring compliance with record retention and disposal schedules and supervising records access and permission controls.

10.6 The **ICT Manager and Department** will be responsible for ensuring that future technologies procured allow access to electronic records for the duration of relevant retention periods.

11. TRAINING AND AWARENESS

11.1 Appropriate training will be made available for existing staff that have responsibility for information governance duties.

11.2 All staff will be made aware of their obligations for information governance through effective communication programmes.

11.3 Each new employee will be made aware of their obligations for information governance during an induction programme.

11.4 Training requirements will be reviewed on a regular basis to take account of the needs of the individual and to ensure that staff are adequately trained.

12. POLICY COMPLIANCE AND AUDIT

12.1 Failure to observe the standards set out in this policy may be regarded as serious and any breach may render an employee liable to disciplinary action, which may include dismissal. The Disciplinary procedure is part of the Local Conditions of Employment. Any disciplinary investigation resulting from a breach of this policy will be undertaken by the line manager.

12.2 Non-compliance with this policy could have a significant effect on efficient operation and may result in financial loss and an inability to provide necessary services to our customers. Academy will undertake audits as required to monitor compliance with its information governance policies.

12.3 Occasionally there may be situations where exceptions to this policy are required, as full adherence may not be practical, could delay business critical initiatives or could increase costs. These will need to be risk assessed on a case-

by-case basis. Where there are justifiable reasons why a particular policy requirement cannot be implemented, a policy exemption may be requested by following the policy exemption process, available here. Exemptions may be granted on a temporary or permanent basis. All exemptions will be subject to review.

12.4 Any user who does not understand the implications of this policy or how it may apply to them should seek advice from their immediate line manager.

13. POLICY GOVERNANCE

13.1 The following table identifies who within the Academy is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups

Responsible	Governing Body
Accountable	Director of Finance & Resources/ICT Manager
Consulted	Senior Leadership Team (SLT)
Informed	All users and persons with management or oversight responsibility for users/staff

14. COMPLAINTS

14.1 Subject to paragraphs 16.2 and 16.3, complaints relating to the Academy's compliance with the UK GDPR will be dealt with in accordance with the Academy's Complaints Policy.

14.2 Complaints relating to access to personal information or access to education records should be made to the DPO who will decide whether it is appropriate for the complaint to be dealt with through the Academy's complaints procedure. Complaints which are not appropriate to be dealt with through the school's

complaints procedure can be referred to the Information Commissioner. Details of how to make a complaint to the ICO will be provided with the response letter.

14.3 Complaints relating to information handling may be referred to the Information Commissioner's Office (the statutory regulator). Contact details can be found on their website at www.ico.org.uk or telephone 01625 5457453.

15. REVIEW AND MAINTENANCE

This policy will be reviewed every two years or sooner if statutory requirements change by the Data Protection Officer, Director of Finance & Resources, and the Principal.

16. ENQUIRIES

Any enquiries in relation to this policy should be directed to the Director of Finance & Resources via the School Office

Further advice and information are available from the Information Commissioner's Office at www.ico.org.uk or telephone 01625 5457453.

17. SUPPORTING POLICIES/DOCUMENTS

Privacy Notice

Secure Destruction Policy

Retention Schedule

SAR Policy

Staff Handbook

Complaints Procedure

Acceptable Use Agreement

18.APPENDIX A

Example of an Academy's Retention Schedule:

Department	Service	Type of file and description	Is there an outstanding SAR/FOI request on these records?	Amount (no. of boxes, files, etc.)	Date of disposal or review	Action taken	Justification	Name of staff member in charge of deletion
Management information system	Generic data management system inc.	Digital records	No	3 files	22.01.2020	Deletion	Staff member left school so removal of details from management system	A.N.Other