



NORTHAMPTON PRIMARY
ACADEMY TRUST PARTNERSHIP

NPAT Records Management Policy, Processes & Schedules

Date approved by the NPAT Board of Trustees:	November 2021
Chair of Trustees Signature:	Jeremy Stockdale
Renewal Date:	November 2024

Background

Section 46 of the Freedom of Information Act 2000 requires schools to follow a Code of Practice on managing their records. Under section 7 of the Code of Practice on the Management of Records, it states that:

"Authorities should have in place a records management policy, either as a separate policy or as part of a wider information or knowledge management policy."

This policy needs to:

- *be endorsed by senior management, for example at board level, and should be readily available to staff at all levels.*
- *provide a mandate for the records and information management function and a framework for supporting standards, procedures and guidelines. The precise contents will depend on the particular needs and culture of the authority, but it should as a minimum:*
 - a) *Set out the authority's commitment to create, keep and manage records which document its principal activities;*
 - b) *Outline the role of records management and its relationship to the authority's overall business strategy;*
 - c) *Identify and make appropriate connections to related policies, such as those dealing with email, information security and data protection;*
 - d) *Define roles and responsibilities, including the responsibility of individuals to document their work in the authority's records to the extent that, and in the way that, the authority has decided their work should be documented, and to use those records appropriately;*
 - e) *Indicate how compliance with the policy and the supporting standards, procedures and guidelines will be monitored.*

The policy should be kept up to date so that it reflects the current needs of the authority. One way of ensuring this is to review it at agreed intervals, for example every three or five years, and after major organisational or technological changes, in order to assess whether it needs amendment.

The authority should consider publishing the policy so that members of the public can see the basis on which it manages its records.

For a full copy of the Lord Chancellor's Code of Practice see <https://www.justice.gov.uk/downloads/information-access-rights/foi/foi-section-46-code-of-practice.pdf>

Northampton Primary Academy Trust (NPAT) 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 institution. Records provide evidence for protecting the legal rights and interests of NPAT and provide evidence for demonstrating performance and accountability. This document provides the policy framework through which this effective management can be achieved and audited. It covers:

- Scope
- Responsibilities
- Relationships with existing policies

Scope of the policy

This policy applies to all records created, received or maintained by staff of NPAT in the course of carrying out their functions.

Records are defined as all those documents which facilitate the business carried out by NPAT 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 electronically.

Responsibilities

NPAT has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The person with overall responsibility for this policy is the NPAT Chief Executive Officer.

The NPAT Data Protection Officer (DPO) will supply guidance for good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and in a timely way. The DPO will also monitor compliance with this policy by surveying at least annually to check if records are stored securely and can be accessed appropriately. Individual staff and employees must ensure that records for which they are responsible are accurate and are maintained and disposed of in accordance with NPAT's records management guidelines.

Records Management Processes & Schedules

Pupil Records

These guidelines are intended to help provide consistency of practice in the way in which pupil records are managed. These will assist our schools about how pupil records should be managed and what kind of information should be included in the file.

These guidelines apply to information created and stored in both physical and electronic format.

These are only guidelines and have no legal status, if you are in doubt about whether a piece of information should be included on the file please contact the Local Authority.

Managing Pupil Records

The pupil record should be seen as the core record charting an individual pupil's progress through the Education System. The pupil record should accompany the pupil to every school they attend and should contain information that is accurate, objective and easy to access. These guidelines are based on the assumption that the pupil record is a principal record and that all information relating to the pupil will be found in the file.

Recording information

Pupils have a right of access to their educational record and so do their parents under the Education (Pupil Information) (England) Regulations 2005. Under the Data Protection Act 1998 a pupil or their nominated representative has a right to see information held about them. This right exists until the point that the file is destroyed. Therefore, it is important to remember that all information should be accurately recorded, objective in nature and expressed in a professional manner.

Primary School records

The pupil record starts its life when a file is opened for each new pupil as they begin school. This is the file which will follow the pupil for the rest of his/her school career

The following information should be easily accessible:

- The name of the pupil's doctor
- Emergency contact details
- Gender
- Preferred name
- Position in family

- Ethnic origin¹
- Language of home (if other than English)²
- Religion³
- Any allergies or other medical conditions that it is important to be aware of⁴
- Names of adults who hold parental responsibility with home address and telephone number (and any additional relevant carers and their relationship to the child)
- Name of the school, admission number and the date of admission and the date of leaving.
- Any other agency involvement e.g. speech and language therapist, paediatrician

It is essential that these files, which contain personal information, are managed against the information security guidelines also contained in the NPAT Records Management Process & Schedule.

1 Although this is “sensitive” data under the Data Protection Act 1998, the Department for Education require statistics about ethnicity

2 This needs to be recorded for the School Census (Mother Tongue)

3 Although this is “sensitive” data under the Data Protection Act 1998, the school has good reasons for collecting the information

4 Although this is “sensitive” data under the Data Protection Act 1998, the school has good reasons for collecting the information

Items which should be included on the pupil record

- If the pupil has attended an early years setting, then the record of transfer should be included on the pupil file
- Admission form (application form)
- Privacy Notice [if these are issued annually only the most recent need be on the file]
- Photography Consents
- Years Record
- Annual Written Report to Parents
- National Curriculum and Religious Education Locally Agreed Syllabus Record Sheets
- Any information relating to a major incident involving the child (either an accident or other incident)
- Any reports written about the child
- Any information about a statement and support offered in relation to the statement
- Any relevant medical information (should be stored in the file clearly marked as such)
- Child protection reports/disclosures (should be stored in the clearly marked as such)
- Any information relating to exclusions (fixed or permanent)
- Any correspondence with parents or outside agencies relating to major issues
- Details of any complaints made by the parents or the pupil

The following records should be stored separately to the pupil record as they are subject to shorter retention periods and if they are placed on the file then it will involve a lot of unnecessary weeding of the files before they are transferred on to another school.

- Absence notes
- Parental consent forms for trips/outings [in the event of a major incident all the parental consent forms should be retained with the incident report not in the pupil record]
- Correspondence with parents about minor issues
- Accident forms (these should be stored separately and retained on the school premises until their statutory retention period is reached. A copy could be placed on the pupil file in the event of a major incident)

Transferring the pupil record to the secondary school

The pupil record should not be weeded before transfer to the secondary school unless any records with a short retention period have been placed in the file. It is important to remember that the information which may seem unnecessary to the person weeding the file may be a vital piece of information required at a later stage.

Primary schools do not need to keep copies of any records in the pupil record except if there is an ongoing legal

action when the pupil leaves the school. Custody of and responsibility for the records passes to the school the pupil transfers to.

Files should not be sent by post unless absolutely necessary. If files are sent by post, they should be sent by registered post with an accompanying list of the files. The secondary school should sign a copy of the list to say that they have received the files and return that to the primary school. Where appropriate, records can be delivered by hand with signed confirmation for tracking and auditing purposes.

Electronic documents that relate to the pupil file also need to be transferred, or, if duplicated in a master paper file, destroyed.

Secondary School records (for information)

Items which should be included on the pupil record

- If the pupil has attended an early years setting, then the record of transfer should be included on the pupil file
- Admission form (application form)
- Privacy Notice [if these are issued annually only the most recent need be on the file]
- Photography Consents
- Years Record
- Annual Written Report to Parents
- National Curriculum and Religious Education Locally Agreed Syllabus Record Sheets
- Any information relating to a major incident involving the child (either an accident or other incident)
- Any reports written about the child
- Any information about a statement and support offered in relation to the statement
- Any relevant medical information (should be stored in the file in a sealed envelope clearly marked as such)
- Child protection reports/disclosures (should be stored in the file in a sealed envelope clearly marked as such)
- Any information relating to exclusions (fixed or permanent)
- Any correspondence with parents or outside agencies relating to major issues
- Details of any complaints made by the parents or the pupil

The following records should be stored separately to the pupil record as they are subject to shorter retention periods and if they are placed on the file then it will involve a lot of unnecessary weeding of the files once the pupil leaves the school.

- Absence notes
- Parental consent forms for trips/outings [in the event of a major incident all the parental consent forms should be retained with the incident report not in the pupil record]
- Correspondence with parents about minor issues
- Accident forms (these should be stored separately and retained on the school premises until their statutory retention period is reached. A copy could be placed on the pupil file in the event of a major incident)

Responsibility for the pupil record once the pupil leaves the school

The school which the pupil attended until statutory school leaving age⁵ is responsible for retaining the pupil record until the pupil reaches the age of 25 years. [See the retention schedule for further information].

Safe destruction of the pupil record

The pupil record should be disposed of in accordance with the safe disposal of records guidelines.

Transfer of a pupil record outside the EU area

If you are requested to transfer a pupil file outside the EU area because a pupil has moved into that area, please contact the NPAT GSRM for further advice.

Storage of pupil records

All pupil records should be kept securely at all times. Paper records, for example, should be kept in lockable storage areas with restricted access, and the contents should be secure within the file. Equally, electronic records should have appropriate security.

Access arrangements for pupil records should ensure that confidentiality is maintained whilst equally enabling information to be shared lawfully and appropriately, and to be accessible for those authorised to see it.

5 Statutory school leaving age was raised to 18 years in 2015.

Good Practice for Managing E-mail

Introduction

These guidelines are intended to assist NPAT staff to manage their e-mail in the most effective way and must be used in conjunction with our policies on the use of ICT.

Information about how your e-mail application works is not included in this document.

Eight Things You Need to Know About E-mail

E-mail has replaced telephone calls and memos.

- As communicating by e-mail is quick and easy, many people have replaced telephone conversations and memos with e-mail discussions. However, the language in which e-mail is written is often less formal and more open to misinterpretation than a written memo or a formal letter. Remember that e-mail should be laid out and formulated to the same professional standards as other written communications.

E-mail is not a secure medium to send confidential information

- You need to think about information security when you send confidential information by e-mail. The consequences of an e-mail containing sensitive information being sent to an unauthorised person could be a civil penalty from the Information Commissioner, in the public domain or with negative publicity. Confidential or sensitive information should only be sent by a secure encrypted e-mail system. Never put personal information (such as a pupil's name) in the subject line of an e-mail.

E-mail is disclosable under the access to information regimes

- All school e-mail is disclosable under Freedom of Information and Data Protection legislation. Be aware that anything you write in an email could potentially be made public.

E-mail is not necessarily deleted immediately

- E-mails can remain in a system for a period of time after you have deleted them. You must remember that although you may have deleted your copy of the e-mail, the recipients may not and therefore there will still be copies in existence. These copies could be disclosable under the Freedom of Information Act or under the Data Protection Act.

E-mail can form a contractual obligation

- Agreements entered into by e-mail can form a contract. You need to be aware of this if you enter into an agreement with anyone, especially external contractors. Individual members of staff should not enter into agreements either with other members of staff internally or with external contractors unless they are

authorised to do so.

E-mail systems are commonly used to store information which should be stored somewhere else

- All attachments in e-mail should be saved into any appropriate electronic filing system or printed out and placed on paper files.

Employers must be careful how they monitor e-mail

- Any employer has a right to monitor the use of e-mail provided it has informed members of staff that it may do so. Monitoring the content of e-mail messages is a more sensitive matter and if you intend to do this you will need to be able to prove that you have the consent of staff. If you intend to monitor staff e-mail or telephone calls you should inform them how you intend to do this and who will carry out the monitoring. The Information Commissioner's Employment Practices Code is an excellent guide to this subject.

E-mail is one of the most common causes of stress in the workplace

- Whilst e-mail can be used to bully or harass people, it is more often the sheer volume of e-mail which causes individuals to feel that they have lost control of their e-mail and their workload. Regular filing and deletion can prevent this happening.

Creating and sending e-mail

Here are some steps to consider when sending e-mail.

Do I need to send this e-mail?

- Ask yourself whether this transaction needs to be done by e-mail? It may be that it is more appropriate to use the telephone or to check with someone face to face.

To whom do I need to send this e-mail?

- Limit recipients to the people who really need to receive the e-mail. Avoid the use of global or group address lists unless it is absolutely necessary. Never send on chain e-mails.

When sending emails containing personal or sensitive data always respond to an authorised, approved address.

- All emails that are used for official business must be sent from an official business domain address.

Use a consistent method of defining a subject line

- Having a clearly defined subject line helps the recipient to sort the e-mail on receipt. A clear subject line also assists in filing all e-mails relating to individual projects in one place. For example, the subject line might be the name of the policy, or the file reference number.

Ensure that the e-mail is clearly written

- Do not use text language or informal language in school e-mails.
- Always sign off with a name (and contact details).
- Make sure that you use plain English and ensure that you have made it clear how you need the recipient to respond.
- Never write a whole e-mail in capital letters. This can be interpreted as shouting.
- Always spell check an e-mail before you send it. Do not use the urgent flag unless it is absolutely necessary, recipients will not respond to the urgent flag if they perceive that you use it routinely.
- If possible, try to stick to one subject for the content of each e-mail, as it will be easier to categorise it later if you need to keep the e-mail.

Sending attachments

Sending large attachments (e.g. graphics or presentations) to a sizeable circulation list can cause resource problems on your network. Where possible put the attachment in an appropriate area on a shared drive and send the link round to the members of staff who need to access it.

Managing received e-mails

This section contains some hints and tips about how to manage incoming e-mails.

Manage interruptions

- Incoming e-mail can be an irritating distraction. The following tips can help manage the interruptions.
- Turn off any alert that informs you e-mail has been received
- Plan times to check e-mail into the day (using an out of office message to tell senders when you will be looking at your e-mail can assist with this).

Use rules and alerts

By using rules and alerts members of staff can manage their inbox into theme-based folders. For example:

- E-mails relating to a specific subject or project can be diverted to a named project folder
- E-mails from individuals can be diverted to a specific folder
- Warn senders that you will assume that if you are copied into an e-mail, the message is for information only and requires no response from you.
- Internally, use a list of defined words to indicate in the subject line what is expected of recipients (for example: "For Action:", FYI:, etc)
- Use electronic calendars to invite people to meetings rather than sending e-mails asking them to attend

Filing e-mail

Attachments only

Where the main purpose of the e-mail is to transfer documents, then the documents should be saved into the appropriate place in an electronic filing system. The e-mail can then be deleted.

E-mail text and attachments

Where the text of the e-mail adds to the context or value of the attached documents it may be necessary to keep the whole e-mail. The best way to do this and retain information which makes up the audit trail, is to save the e-mail in .pdf format. This can be done within Outlook and saved to the appropriate place in the electronic filing system.

E-mail text only

If the text in the body of the e-mail requires filing, the same method can be used as that outlined above. This will retain information for audit trail purposes.

How long to keep e-mails?

E-mail is primarily a communications tool, and e-mail applications are not designed for keeping e-mail as a record.

Safe disposal of records which have reached the end of their administrative life

NB: Please be aware that this guidance applies to all types of record, whether they are in paper or digital format.

Disposal of records that have reached the end of the minimum retention period allocated

The fifth data protection principle states that:

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes

We must ensure that records that are no longer required for business use are reviewed as soon as possible under

the criteria set out so that only the appropriate records are destroyed.

Individual academies will determine whether records are to be selected for permanent preservation, destroyed, digitised to an electronic format or retained by the organisation for research or litigation purposes.

Refer to the Retention Guidelines at the end of the toolkit.

Safe destruction of records

All records containing personal information, or sensitive policy information should be made either unreadable or unreconstructable.

- Paper records should be shredded using a cross-cutting shredder
- CDs / DVDs / Floppy Disks should be cut into pieces
- Audio / Video Tapes and Fax Rolls should be dismantled and shredded
- Hard Disks should be dismantled and sanded

Any other records should be bundled up and disposed in other appropriate ways.

Where an external provider is used it is recommended that all records must be shredded on-site in the presence of an employee. The organisation must also be able to prove that the records have been destroyed by the company who should provide a Certificate of Destruction. Staff working for the external provider should have been trained in the handling of confidential documents.

It is important to understand that if the records are recorded as to be destroyed but have not yet been destroyed and a request for the records has been received, they MUST still be provided. Records should be shredded as soon as the record has been documented as being destroyed.

Freedom of Information Act 2000 (FoIA 2000)

The Freedom of Information Act 2000 requires the school to maintain a list of records which have been destroyed and who authorised their destruction. Members of staff should record at least:

- File reference (or other unique identifier);
- File title (or brief description);
- Number of files and date range
- The name of the authorising officer
- Date action taken

Following this guidance will ensure that the school is compliant with the Data Protection Act 1998 and the Freedom of Information Act 2000.

Appropriate Storage for Physical Records

Records must be stored in the workplace in a way that does not cause a health and Safety hazard. Records must not be stored in corridors or gangways and must not impede or block fire exits. There should be where appropriate, heat/smoke detectors connected to fire alarms, a sprinkler system and the required number of fire extinguishers. The area should be secured against intruders and have controlled access as far as possible to the working space.

Storage areas should be regularly monitored and checked for any damage or emerging risks, especially during holiday periods.

The following are hazards which need to be considered before approving areas where physical records can be stored.

Environmental Damage - Fire

Records can be damaged beyond repair by fire. Smoke and water damage will also occur to records which have been in a fire, although generally records damaged by smoke or water can be repaired.

Core records should be kept in cabinets or cupboards. Metal filing cabinets will usually suffice, but for important core records, fireproof cabinets may need to be considered. However, fireproof cabinets are expensive and very heavy so they should only be used in special circumstances.

Environmental Damage - Water

Records damaged by water can sometimes be repaired by a specialist document salvage company. The salvage process is expensive; therefore, records need to be protected against water damage where possible. Where flooding is involved, the water may not always be clean and records could become contaminated as well as damaged.

Records should not be stored directly under water pipes or in places which are liable to flooding (either from excess rainfall or from the overflow of toilet cisterns). Records should be stored in cabinets/cupboards with tight fitting doors which provide protection from water ingress. Records stored on desks or in cabinets/cupboards without close fitting doors will suffer serious water damage.

Records should be stored at least 2 inches off the ground. Most office furniture stands 2 inches off the ground. Portable storage containers (i.e. boxes or individual filing drawers) should be raised off the ground by at least 2 inches. This is to ensure that in the case of a flood that records are protected against immediate flood damage.

Storage areas should be checked for possible damage after extreme weather to ensure no water ingress has occurred.

Environmental Damage – Sunlight

Records should not be stored in direct sunlight (e.g. in front of a window). Direct sunlight will cause records to fade and the direct heat causes paper to dry out and become brittle.

Environmental Damage – High Levels of Humidity

Records should not be stored in areas which are subject to high levels of humidity. Excess moisture in the air can result in mould forming on the records. Mould can be a hazard to human health and will damage records often beyond repair.

The temperature in record storage areas should not exceed 18°C and the relative humidity should be between 45% and 65%.

Storage areas should be checked for damage after extreme weather conditions to reduce the risk of mould growth.

Environmental Damage – Insect/Rodent Infestation

Records should not be stored in areas which are subject to insect infestation or which have a rodent problem (rats or mice).

Retention Guidelines

The purpose of the retention guidelines

Under the Freedom of Information Act 2000, schools are required to maintain a retention schedule listing the record series which the school creates in the course of its business. The retention schedule lays down the length of time which the record needs to be retained and the action which should be taken when it is of no further administrative use. The retention schedule lays down the basis for normal processing under both the Data Protection Act 1998 and the Freedom of Information Act 2000.

Members of staff are expected to manage their current record keeping systems using the retention schedule and to take account of the different kinds of retention periods when they are creating new record keeping systems.

The retention schedule refers to record series regardless of the media in which they are stored.

Benefits of a retention schedule

There are a number of benefits which arise from the use of a complete retention schedule:

- Managing records against the retention schedule is deemed to be “normal processing” under the Data Protection Act 1998 and the Freedom of Information Act 2000. Members of staff should be aware that once a Freedom of Information request is received or a legal hold imposed then records disposal relating to the request or legal hold must be stopped.
- Members of staff can be confident about safe disposal information at the appropriate time.
- Information which is subject to Freedom of Information and Data Protection legislation will be available when required. The school is not maintaining and storing information unnecessarily.

Maintaining and amending the retention schedule

Where appropriate the retention schedule should be reviewed and amended to include any new record series created and remove any obsolete record series.

This retention schedule contains recommended retention periods for the different record series created and maintained by schools in the course of their business. The schedule refers to all information regardless of the media in which it is stored.

Some of the retention periods are governed by statute. Others are guidelines following best practice. Every effort has been made to ensure that these retention periods are compliant with the requirements of the Data Protection Act 1998 and the Freedom of Information Act 2000.

Managing record series using these retention guidelines will be deemed to be “normal processing” under the legislation mentioned above.

Using the Retention Schedule

The Retention Schedule is divided into sections:

- Management of the School
- Human Resources
- Financial Management of the School
- Property Management
- Pupil Management
- Curriculum Management

- Extra-Curricular Activities
- Central Government and Local Authority

Management of the School

This section contains retention periods connected to the general management of the school. This covers the work of the Board of Trustees and all sub-committees, the Executive team, the admissions process and operational administration.

1.1 Governing Body					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.1.1	Agendas for Governing Body meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff		One copy should be retained with the master set of minutes. All other copies can be disposed of	SECURE DISPOSAL ¹
1.1.2	Minutes of Governing Body meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff			
	Principal Set (signed)			PERMANENT	
	Inspection Copies ²			Date of meeting + 3 years	If these minutes contain any sensitive, personal information they must be shredded.
1.1.3	Reports presented to the Governing Body	There may be data protection issues if the report deals with confidential issues		Reports should be kept for a minimum of 6 years. However, if the minutes refer directly to individual reports then the reports should be kept	SECURE DISPOSAL or retain with the signed set of the minutes

¹ In this context SECURE DISPOSAL should be taken to mean disposal using confidential waste bins, or if the school has the facility, shredding using a cross cut shredder.

² These are the copies which the clerk to the Governor may wish to retain so that requestors can view all the appropriate information without the clerk needing to print off and collate redacted copies of the minutes each time a request is made.

1.1 Governing Body					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.1.5	Instruments of Government including Articles of Association	No		PERMANENT	These should be retained in the school
1.1.6	Trusts and Endowments managed by the Governing Body	No		PERMANENT	These should be retained in the school
1.1.7	Action plans created and administered by the Governing Body	No		Life of the action plan + 3 years	SECURE DISPOSAL
1.1.8	Policy documents created and administered by the Governing	No		Life of the policy + 3 years	SECURE DISPOSAL
1.1.9	Records relating to complaints dealt with by the Governing Body	Yes		Date of the resolution of the complaint + a minimum of 6 years then review for further retention in case of contentious	SECURE DISPOSAL
1.1.10	Proposals concerning the change of status of a maintained school including Specialist Status Schools and Academies	No		Date proposal accepted or declined + 3 years	SECURE DISPOSAL

Please note that all information about the retention of records concerning the recruitment of Headteachers and Executive Team can be found in the Human Resources section below.

1.2 Headteachers and Executive Team					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.2.1	Log books of activity in the school maintained by the Headteachers	There may be data protection issues if the log book refers to individual pupils or members of staff		Date of last entry in the book + a minimum of 6 years then review	SECURE DISPOSAL
1.2.2	Minutes of Executive Team meetings and the meetings of other internal administrative bodies	There may be data protection issues if the minutes refer to individual pupils or members of staff		Date of the meeting + 3 years then review	SECURE DISPOSAL
1.2.3	Reports created by the Headteachers or the Executive Team	There may be data protection issues if the report refers to individual pupils or members of staff		Date of the report + a minimum of 3 years then review	SECURE DISPOSAL
1.2.4	Records created by Headteachers, deputy Headteachers, heads of year/house and other members	There may be data protection issues if the records refer to individual pupils or members of staff		Current academic year + 6 years then review	SECURE DISPOSAL
1.2.5	Correspondence created by Headteachers, deputy Headteachers, heads of year/house and other members of staff with administrative responsibilities	There may be data protection issues if the correspondence refers to individual pupils or members of staff		Date of correspondence + 3 years then review	SECURE DISPOSAL
1.2.6	Professional Development Plans	Yes		Life of the plan + 6 years	SECURE DISPOSAL
1.2.7	School Development Plans	No		Life of the plan + 3 years	SECURE DISPOSAL

1.4 Operational Administration					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.4.1	General filing	No		Current year + 5 years then REVIEW	SECURE DISPOSAL
1.4.2	Records relating to the creation and publication of the school brochure or prospectus	No		Current year + 3 years	STANDARD DISPOSAL
1.4.3	Records relating to the creation and distribution of circulars to staff, parents or pupils	No		Current year + 1 year	STANDARD DISPOSAL
1.4.4	Newsletters and other items with a short operational use	No		Current year + 1 year	STANDARD DISPOSAL
1.4.5	Visitors' Books and Signing in Sheets	Yes		Current year + 6 years then REVIEW	SECURE DISPOSAL
1.4.6	Records relating to the creation and management of Parent Teacher Associations and/or Old Pupils Associations	No		Current year + 6 years then REVIEW	SECURE DISPOSAL
1.4.7	All other records with short operational use including broadcast items, films produced, and other media recordings	Yes	Data Protection Act	Current year + 1 year	SECURE DISPOSAL

2. Human Resources

This section deals with all matters of Human Resources management within the school.

2.1 Recruitment					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the
2.1.1	All records leading up to the appointment of a new Headteacher	Yes		Date of appointment + 6 years	SECURE DISPOSAL
2.1.2	All records leading up to the appointment of a new member of staff – unsuccessful candidates	Yes		Date of appointment of successful candidate + 6 months	SECURE DISPOSAL
2.1.3	All records leading up to the appointment of a new member of staff – successful candidate	Yes		All the relevant information should be added to the staff personal file (see below) and all other information retained for 6 months	SECURE DISPOSAL
2.1.4	Pre-employment vetting information – DBS Checks	No	DBS Update Service Employer Guide June 2014: Keeping children Safe in education. July 2015 (Statutory Guidance from DfE) Sections 73, 74		SECURE DISPOSAL
2.1.5	Proofs of identity collected as part of the process of checking “portable” enhanced DBS disclosure	Yes		Where possible these should be checked and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation then this should be placed on the member of staff’s personal file	SECURE DISPOSAL
2.1.6	Pre-employment vetting information – Evidence proving the right to work in the United Kingdom ⁴	Yes	An employer’s guide to right to work checks [Home Office May 2015]	Where possible these documents should be added to the Staff Personal File [see below], but if they are kept separately then the Home Office requires that the documents are kept for termination of Employment plus not less than two years	SECURE DISPOSAL

2.2 Operational Staff Management

	Basic file description	Data Prot Issue	Statutory Provisions	Retention Period [Operational] administrative	Action at the end of the
2.2.1	Staff Personal File	Yes	Limitation Act 1980 (Section 2)	Termination of Employment + 6 years	SECURE DISPOSAL
2.2.2	Timesheets	Yes		Current year + 6 years	SECURE DISPOSAL
2.2.3	Annual appraisal/ assessment records	Yes		Current year + 5 years	SECURE DISPOSAL

2.3 Management of Disciplinary and Grievance Processes

	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.3.1	Allegation of a child protection nature against a member of staff including where the allegation is unfounded ⁵	Yes	"Keeping children Safe in education Statutory guidance for schools and colleges March 2015"; "Working together to Safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer then REVIEW. Note allegations that are found to be malicious should be removed from personnel files. If found they are to be kept on the file and a copy provided to the person concerned	SECURE DISPOSAL These records must be shredded
2.3.2	Disciplinary Proceedings	Yes			
	oral warning			Date of warning + 6 months	
	written warning – level 1			Date of warning + 6 months	SECURE DISPOSAL
	written warning – level 2			Date of warning + 12 months	[If warnings are placed on personal files then they must be weeded from the file]
	final warning			Date of warning + 18 months	
	case not found			If the incident is child protection related then see above otherwise dispose of at the conclusion of the	SECURE DISPOSAL

2.4 Health and Safety					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.4.1	Health and Safety Policy Statements	No		Life of policy + 3 years	SECURE DISPOSAL
2.4.2	Health and Safety Risk Assessments	No		Life of risk assessment + 3 years	SECURE DISPOSAL
2.4.3	Records relating to accident/ injury at work	Yes		Date of incident + 12 years In the case of serious accidents a further retention period will need to be applied	SECURE DISPOSAL
2.4.4	Accident Reporting	Yes	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980		
	Adults			Date of the incident + 6 years	SECURE DISPOSAL
	Children			DOB of the child + 25 years	SECURE DISPOSAL
2.4.5	Control of Substances Hazardous to Health (COSHH)	No	Control of Substances Hazardous to Health Regulations 2002. SI 2002 No 2677 Regulation 11; Records kept under the 1994 and 1999 Regulations to be kept as if the 2002 Regulations had not been made. Regulation 18 (2)	Current year + 40 years	SECURE DISPOSAL
2.4.6	Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos	No	Control of Asbestos at Work Regulations 2012 SI 1012 No 632 Regulation 19	Last action + 40 years	SECURE DISPOSAL
2.4.7	Process of monitoring of areas where employees and persons are likely to have become in contact with radiation	No		Last action + 50 years	SECURE DISPOSAL

2.4.8 Fire Precautions logbooks	No		Current year + 6 years	SECURE DISPOSAL
---------------------------------	----	--	------------------------	-----------------

2.5 Payroll and Pensions					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.5.1	Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI1986/1960), revised 1999 (SI1999/567)	Current year + 3 years	SECURE DISPOSAL
2.5.2	Records held under Retirement Benefits Schemes (Information Powers)	Yes		Current year + 6 years	SECURE DISPOSAL

3. Financial Management of the School

This section deals with all aspects of the financial management of the school including the administration of school meals.

3.1 Risk Management and Insurance					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.1.1	Employer's Liability Insurance Certificate	No		Closure of the school + 40 years	SECURE DISPOSAL

3.2 Asset Management					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.2.1	Inventories of furniture and equipment	No		Current year + 6 years	SECURE DISPOSAL
3.2.2	Burglary, theft and vandalism report forms	No		Current year + 6 years	SECURE DISPOSAL

³ This review took place as the Independent Inquiry on Child Sexual Abuse was beginning. In light of this, it is recommended that all records relating to child abuse are retained until the Inquiry is completed. This section will then be reviewed again to take into account any recommendations the Inquiry might make concerning record retention

⁴ Where the warning relates to child protection issues see above. If the disciplinary proceedings relate to a child protection matter please contact your Safeguarding Children Officer for further advice

3.3 Accounts and Statements including Budget Management					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.3.1	Annual Accounts	No		Current year + 6 years	STANDARD DISPOSAL
3.3.2	Loans and grants managed by the school	No		Date of last payment on the loan + 12 years then REVIEW	SECURE DISPOSAL
3.3.3	Student Grant applications	Yes		Current year + 3 years	SECURE DISPOSAL
3.3.4	All records relating to the creation and management of budgets including the Annual Budget statement and background papers	No		Life of the budget + 3 years	SECURE DISPOSAL
3.3.5	Invoices, receipts, order books and requisitions, delivery notices	No		Current financial year + 6 years	SECURE DISPOSAL
3.3.6	Records relating to the collection and banking of monies	No		Current financial year + 6 years	SECURE DISPOSAL
3.3.7	Records relating to the identification and collection of debt	No		Current financial year + 6 years	SECURE DISPOSAL

3.4 Contract Management					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.4.1	All records relating to the management of contracts under seal	No	Limitation Act 1980	Last payment on the contract + 12 years	SECURE DISPOSAL
3.4.2	All records relating to the management of contracts under signature	No	Limitation Act 1980	Last payment on the contract + 6 years	SECURE DISPOSAL
3.4.3	Records relating to the monitoring of contracts	No		Current year + 2 years	SECURE DISPOSAL

3.5 School Fund					
	Basic file description	Data Prot	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.5.1	School Fund - Cheque books	No		Current year + 6 years	SECURE DISPOSAL
3.5.2	School Fund - Paying in books	No		Current year + 6 years	SECURE DISPOSAL
3.5.3	School Fund – Ledger	No		Current year + 6 years	SECURE DISPOSAL
3.5.4	School Fund – Invoices	No		Current year + 6 years	SECURE DISPOSAL
3.5.5	School Fund – Receipts	No		Current year + 6 years	SECURE DISPOSAL
3.5.6	School Fund - Bank statements	No		Current year + 6 years	SECURE DISPOSAL
3.5.7	School Fund – Journey Books	No		Current year + 6 years	SECURE DISPOSAL

3.6 School Meals Management					
	Basic file description	Data Prot	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.6.1	Free School Meals Registers	Yes		Current year + 6 years	SECURE DISPOSAL
3.6.2	School Meals Registers	Yes		Current year + 3 years	SECURE DISPOSAL
3.6.3	School Meals Summary Sheets	No		Current year + 3 years	SECURE DISPOSAL

4. Property Management

This section covers the management of buildings and property.

4.1 Property Management					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the
4.1.1	Title deeds of properties belonging to the school	No		PERMANENT These should follow the property unless the property has been registered with the Land Registry	
4.1.2	Plans of property belong to the school	No		These should be retained whilst the building belongs to the school and should be passed onto any new owners if the building is leased or sold.	
4.1.3	Leases of property leased by or to the school	No		Expiry of lease + 6 years	SECURE DISPOSAL
4.1.4	Records relating to the letting of school premises	No		Current financial year + 6 years	SECURE DISPOSAL

4.2 Maintenance					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the
4.2.1	All records relating to the maintenance of the school carried out by contractors	No		Current year + 6 years	SECURE DISPOSAL
4.2.2	All records relating to the maintenance of the school carried out by school employees including maintenance log books	No		Current year + 6 years	SECURE DISPOSAL

5. Pupil Management

This section includes all records which are created during the time a pupil spends at the school. For information about accident reporting see under Health and NPATety above.

5.1 Pupil's Educational Record					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
5.1.1	Pupil's Educational Record required by The Education (Pupil Information) (England) Regulations 2005	Yes	The Education (Pupil Information) (England) Regulations 2005 SI 2005 No. 1437		
	Primary			Retain whilst the child remains at the primary school	<p>The file should follow the pupil when he/she leaves the primary school. This will include:</p> <ul style="list-style-type: none"> • to another primary school • to a secondary school • to a pupil referral unit <p>If the pupil dies whilst at primary school the file should be retained for the statutory retention period.</p> <p>If the pupil transfers to an independent school, transfers to home schooling or leaves the country the file should be retained for the statutory retention period. Primary Schools do not ordinarily have sufficient storage space to store records for pupils who have not transferred in the normal way.</p>
	Secondary (for info)		Limitation Act 1980 (Section 2)	Date of Birth of the pupil + 25 years	SECURE DISPOSAL
5.1.2	Examination Results – Pupil Copies	Yes			
	Public			This information should be added to the pupil file	All uncollected certificates should be returned to the examination board.
	Internal			This information should be added to the pupil file	

5.1 Pupil's Educational Record

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
This review took place as the Independent Inquiry on Child Sexual Abuse was underway. In light of this, it is recommended that all records relating to child abuse are retained until the Inquiry is completed. This section will then be reviewed again to take into account any recommendations the Inquiry might make concerning record retention				
5.1.3 Child Protection information held pupil file	Yes	"Keeping children Safe in education Statutory guidance for schools and colleges March 2015"; "Working together to Safeguard children. A guide to inter-agency working to Safeguard and promote the welfare of children March 2015"	If any records relating to child protection issues are placed on the pupil file, it should be in a sealed envelope and then retained for the same period of time as the pupil file.	SECURE DISPOSAL – these records MUST be shredded
5.1.4 Child protection information held in separate files	Yes	"Keeping children Safe in education Statutory guidance for schools and colleges March 2015"; "Working together to Safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	DOB of the child + 25 years then review This retention period was agreed in consultation with the Safeguarding Children Group on the understanding that the principal copy of this information will be found on the Local Authority Social Services record	SECURE DISPOSAL – these records MUST be shredded

Retention periods relating to allegations made against adults can be found in the Human Resources section of this retention schedule.

5.2 Attendance					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
5.2.1	Attendance Registers	Yes	School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities October 2014	Every entry in the attendance register must be preserved for a period of three years after the date on which the entry was made.	SECURE DISPOSAL
5.2.2	Correspondence relating to authorized absence		Education Act 1996 Section 7	Current academic year + 2 years	SECURE DISPOSAL

5.3 Special Educational Needs					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
5.3.1	Special Educational Needs files, reviews and Individual Education Plans	Yes	Limitation Act 1980 (Section 2)	Date of Birth of the pupil + 25 years	REVIEW NOTE: This retention period is the minimum retention period that any pupil file should be kept. Some authorities choose to keep SEN files for a longer period of time to defend themselves in a "failure to provide a sufficient education" case. There is an element of business risk analysis involved in any decision to keep the records longer than the minimum retention period and this should be documented.
5.3.2	Statement maintained under section 234 of the Education Act 1990 and any amendments made to the statement	Yes	Education Act 1996 Special Educational Needs and Disability Act 2001 Section 1	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold
5.3.3	Advice and information provided to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold
5.3.4	Accessibility Strategy	Yes	Special Educational Needs and Disability Act 2001 Section 14	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold

6. Curriculum Management

6.1 Statistics and Management Information					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the
6.1.1	Curriculum returns	No		Current year + 3 years	SECURE DISPOSAL
6.1.2	Examination Results (Schools Copy)	Yes		Current year + 6 years	SECURE DISPOSAL
	SATS records –	Yes			
	Results			The SATS results should be recorded on the pupil's educational file and will therefore be retained until the pupil reaches the age of 25 years. The school may wish to keep a composite record of all the whole year SATs results. These could be kept for current year + 6 years to allow suitable comparison	SECURE DISPOSAL
	Examination Papers			The examination papers should be kept until any appeals/validation process is complete	SECURE DISPOSAL
6.1.3	Published Admission Number (PAN)	Yes		Current year + 6 years	SECURE DISPOSAL
6.1.4	Value Added and Contextual	Yes		Current year + 6 years	SECURE DISPOSAL
6.1.5	Self-Evaluation Forms	Yes		Current year + 6 years	SECURE DISPOSAL

6.2 Implementation of Curriculum					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
6.2.1	Schemes of Work	No		Current year + 1 year	
6.2.2	Timetable	No		Current year + 1 year	
6.2.3	Class Record Books	No		Current year + 1 year	
6.2.4	Mark Books	No		Current year + 1 year	
6.2.5	Record of homework set	No		Current year + 1 year	
6.2.6	Pupils' Work	No		Where possible pupils' work should be returned to the pupil at the end of the academic year if this is not the school's policy then current year + 1 year	SECURE DISPOSAL

7. Extra Curricular & Enrichment Activities

7.1 Educational Visits outside the Classroom					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the
7.1.1	Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Primary	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 - "Legal Framework and Employer Systems" and Section 4 - "Good Practice".	Date of visit + 14 years	SECURE DISPOSAL
7.1.2	Records created by schools to obtain approval to run an Educational Visit outside the	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 - "Legal Framework and Employer Systems" and Section 4 - "Good Practice".	Date of visit + 10 years	SECURE DISPOSAL
7.1.3	Parental consent forms for school trips where there has been no major incident	Yes		Conclusion of the trip + 3 years	Although the consent forms could be retained for DOB + 22 years, the requirement for them being needed is low and most schools do not have the storage capacity to retain every single consent form issued by the school for this period of time.
7.1.4	Parental permission slips for school trips – where there has been a major incident	Yes	Limitation Act 1980 (Section 2)	DOB of the pupil involved in the incident + 25 years The permission slips for all the pupils on the trip need to be retained to show that the rules had been followed for all pupils	

					SECURE DISPOSAL
7.1.5	All additional records including photographs, film, voice recording and other media forms	Yes	Data Protection Act	Current year + 1 year	

7.2 Walking Bus					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
7.2.1	Walking Bus Registers	Yes		Date of register + 3 years This takes into account the fact that if there is an incident requiring an accident report the register will be submitted with the accident report and kept for the period of time required for accident reporting	SECURE DISPOSAL

7.3 Family Liaison Officers and Home School Liaison Assistants					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
7.3.1	Day Books	Yes		Current year + 2 years then review	
7.3.2	Reports for outside agencies - where the report has been included on the case file created by the outside agency	Yes		Whilst child is attending school and then destroy	
7.3.3	Referral forms	Yes		While the referral is current	
7.3.4	Contact data sheets	Yes		Current year then review, if contact is no longer active then destroy	
7.3.5	Contact database entries	Yes		Current year then review, if contact is no longer active then destroy	
7.3.6	Group Registers	Yes		Current year + 2 years	

8. Central Government and Local Authority

8.2 Central Government					
Basic file description		Data Prot Issues	Statutory Provision	Retention Period [Operational]	Action at the end of the administrative life of the record
8.2.1 OFSTED reports and papers		No		Life of the report then REVIEW	SECURE DISPOSAL
8.2.2 Returns made to central government		No		Current year + 6 years	SECURE DISPOSAL
8.2.3 Circulars and other information sent from central government		No		Operational use	SECURE DISPOSAL

8.1 Local Authority					
Basic file description		Data Prot Issues	Statutory Provision	Retention Period [Operational]	Action at the end of the administrative life of the record
8.1.1 Secondary Transfer Sheets (Primary)			Yes	Current year + 2 years	SECURE DISPOSAL
8.1.2 Attendance Returns			Yes	Current year + 1 year	SECURE DISPOSAL
8.1.3 School Census Returns			No	Current year + 5 years	SECURE DISPOSAL
8.1.4 Circulars and other information sent from the Local Authority			No	Operational use	SECURE DISPOSAL