



GDPR Documentation Management Policy

CEO Approval: November 2026

Review Date: January 2028

Contents

1.	About this policy.....	4
2.	Scope	4
3.	Legislation and Guidance.....	4
4.	Responsibilities.....	5
5.	Safe destruction of records	5
6.	Freedom of Information Act 2000.....	6
7.	Management of pupil records	6
8.	Retention of pupil records and other pupil-related information	8
	➤ Pupil Admissions Process	9
	➤ Pupils Educational Record	9
	➤ Pupil Attendance.....	10
	➤ Special Educational Needs	10
9.	Curriculum management and Extra-curricular Activities	10
	➤ Statistics and Management Information.....	10
	➤ Implementation of the Curriculum	11
	➤ School Trips.....	12
	➤ Organisations and Groups that support the school	12
10.	Retention of staff records.....	13
	➤ Operational	14
	➤ Recruitment	15
	➤ Disciplinary and grievance procedures	16
11.	Retention of senior leadership and management records	17
	➤ Governance Records	18
	➤ CEO/Head and senior leadership team (SLT)	20
12.	Retention of health and safety records	20
	➤ Health and Safety.....	21
13.	Retention of financial records.....	22
	➤ Payroll and pensions	22
	➤ Risk management and insurance	22
	➤ Asset management	23

➤ Accounts and statements including budget management	23
➤ Contract management	23
➤ School meals.....	24
14. Retention of other school records.....	24
➤ Property management	24
➤ Maintenance.....	24
➤ Government & LA Returns.....	25
➤ Operational administration	25
15. Storing and protecting information.....	25
16. Accessing information	27
17. Digital continuity statement	28
18. Information audit.....	28
19. Disposal of data	29
20. Monitoring and review.....	30

1. About this policy

Prime7 MAT recognises that by efficiently managing our records, we will be able to comply with our legal and regulatory obligations, and to contribute to the effective overall management of our Trust and individual schools. Maintaining good records helps us to provide the evidence needed to protect the legal rights and interests of our school, and for us to demonstrate our performance and accountability.

This policy provides the framework through which we will effectively manage our records.

It covers:

- Scope
- Responsibilities
- Safe destruction of records
- Freedom of Information Act 2000
- Relationships with existing policies

2. Scope

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

Records are defined as all documents which facilitate the business carried out by the Trust and individual schools and which are thereafter retained to provide evidence of transactions or activities. These records may be created, received or maintained in hard copy or electrical format e.g. paper documents, scanned documents, e-mails, audio and video recordings, text messages, notes of telephone and spreadsheets, Word Documents, presentations, etc.

3. Legislation and Guidance

This policy meets the requirements of the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA 2018) and the Freedom of Information Act 2000 (FOIA 2000). It is based on the IRMS Toolkit For Schools, the Department of Education – Data Protection Toolkit for Schools, Department of Education – Annual Review of School Records and Safe Destruction Checklist, and guidance published by the Information Commissioner’s Office (ICO) on the GDPR.

4. Responsibilities

- The Trust as a whole has a statutory responsibility to maintain its records and record-keeping systems in accordance with the regulatory framework.
- The CEO holds overall responsibility for this policy and for ensuring it is implemented correctly.
- The CFO, who is the Data Protection Officer (DPO) for the Trust, will provide guidance on good records management practices and will promote compliance with this policy so that information will be retrieved easily, appropriately and in a timely way.
- The DPO is responsible for ensuring that all records are stored securely, in accordance with the retention periods outlined in this policy and are disposed of correctly. The DPO will monitor compliance with this policy by ensuring that the 'Annual Review of School Records Checklist' is completed at least annually.
- All staff members are responsible for ensuring that the trust does not keep personal information for longer than is necessary for the purpose or purposes for which it was collected. It is the responsibility of all members of the Trust to ensure that they:
 - Manage school records consistently in accordance with school's policies and procedures;
 - Properly document their actions and decisions;
 - Hold personal information securely;
 - Only share personal information appropriately and do not disclose it to an unauthorised third party;
 - Dispose of records securely in accordance with the guidance set out in the Information and Records Management Society's toolkit for schools/ school's Records Retention Schedule which can be found [here](#);
- Staff who do not comply with this policy may face disciplinary action.
- This policy does not form part of any employee's contract of employment and may be amended at any time.

5. Safe destruction of records

- All records containing personal information, or sensitive policy information will 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 will be bundled up and disposed of to a wastepaper merchant or disposed of in other appropriate ways.
- Do not put records containing personal information with the regular waste or a skip.
- Where an external provider is used, where possible, all records will 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 will be trained in the handling of confidential documents.
- The shredding will be planned with specific dates and all records will be identified as to the date of destruction.

Please Note: 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.

6. Freedom of Information Act 2000

The Freedom of Information Act 2000 requires us to maintain a list of records which have been destroyed and who authorised their destruction

When destroying either a substantial amount of information or information which is of a particularly sensitive or important nature, members of staff should record at least:

- The information that has been destroyed
- The volume of the information that has been destroyed
- Who provided authorisation to destroy the information
- The date the information was destroyed

By following this guidance and completing the Annual Checklist, we will ensure that our Trust is compliant with the Data Protection rules and the Freedom of Information Act 2000.

This policy will be implemented in accordance with the following trust policies and procedures:

- Data Protection Policy
- Freedom of Information Policy
- E-security Policy

7. Management of pupil records

- Pupil records are specific documents that are used throughout a pupil’s time in the education system – they are passed to each school that a pupil attends and includes all personal

information relating to them, e.g. date of birth, home address, as well as their progress and achievement.

- The following information is stored on the front of a pupil record and electronically on the school's MIS and will be easily accessible:
 - Forename, surname,
- The following information is stored inside the front cover of a pupil record and electronically on the school's MIS and will be easily accessible:
 - Ethnic origin, religion and first language (if not English)
 - Any preferred names
 - Position in their family, e.g. eldest sibling
 - Emergency contact details and the name of the pupil's doctor
 - Any allergies or other medical conditions that are important to be aware of
 - Names of parents, including their home address(es) and telephone number(s)
 - Name of the school, admission number, the date of admission and the date of leaving, where appropriate
 - Any other agency involvement, e.g. speech and language therapist

The following information is stored in a pupil record, and will be easily accessible:

- Admissions form
- Details of any SEND
- If the pupil has attended an early years setting, the record of transfer
- Fair processing notice – only the most recent notice will be included
- Annual written reports to parents
- National curriculum and agreed syllabus record sheets
- Notes relating to major incidents and accidents involving the pupil
- Any information about an education and healthcare plan (EHCP) and support offered in relation to the EHCP
- Any notes indicating child protection disclosures and reports are held
- Any information relating to exclusions
- Any correspondence with parents or external agencies relating to major issues, e.g. mental health
- Notes indicating that records of complaints made by parents or the pupil are held

The following information is subject to shorter retention periods and, therefore, will be stored separately in a personal file for the pupil in the school office:

- Absence notes
 - Parental and, where appropriate, pupil consent forms for educational visits, photographs and videos, etc.
 - Correspondence with parents about minor issues, e.g. behaviour
-
- Hard copies of disclosures and reports relating to child protection are stored in a sealed envelope, in a securely locked filing cabinet in accordance with each school's Safeguarding lead— a note indicating this is marked on the pupil's file.
 - Hard copies of complaints made by parents or pupils are stored in a file in the Heads Office – a note indicating this is marked on the pupil's file.
 - Actual copies of accident and incident information are stored in the pupil's file in the event of a major accident or incident.
 - The school will ensure that no pupil records are altered or amended before transferring them to the next school that the pupil will attend.
 - The only exception to the above is if any records placed on the pupil's file have a shorter retention period and may need to be removed. In such cases, the DPO responsible for disposing records, will remove these records.
 - Electronic records relating to a pupil's record will also be transferred to the pupils' next school.
 - If any pupil attends the school until statutory school leaving age, the school will keep the pupil's records until the pupil reaches the age of 25 years.
 - The school will, wherever possible, avoid sending a pupil record by post. Where a pupil record must be sent by post, it will be sent by registered post, with an accompanying list of the files included. The school it is sent to is required to sign a copy of the list to indicate that they have received the files and return this to the school.

8. Retention of pupil records and other pupil-related information

The table below outlines the school's retention periods for individual pupil records and the action that will be taken after the retention period, in line with any requirements.

Electronic copies of any information and files will be destroyed in line with the retention periods below.

Pupil Admissions Process			
Type of file	Personal Information	Retention period	Action taken after retention period ends
All records relating to the creation and implementation of the School Admissions Policy	No	Life of the policy + 7 years then review	Secure disposal
Register of admissions	Yes	3 years after the date on which the entry was made	Secure disposal
Primary school admissions – if the admission is successful	Yes	Date of admission + 1 year	Secure disposal
Admissions – if the appeal is unsuccessful	Yes	Resolution of case + 1 year	Secure disposal
Proof of address (supplied as part of the admissions process)	Yes	The current academic year + 1 year	Secure disposal
Supplementary information submitted, including religious and medical information etc. – successful admissions	Yes	Added to the pupil's record	Secure disposal
Supplementary information submitted, including religious and medical information etc. – unsuccessful admissions	Yes	Until appeals process completed	Secure disposal

Pupils Educational Record			
Type of file	Personal Information	Retention period	Action taken after retention period ends
Primary Pupil's educational record required by The Education (Pupil Information) (England) Regulations 2005	Yes	Whilst the pupil remains at the school	Transferred to the next destination when the pupil leaves the primary school
Child protection information held on a pupil's record	Yes	Stored in a sealed envelope for the same length of time as the pupil's record	Secure disposal – must be shredded

Child protection records held in a separate file	Yes	DOB of the child + 25 years then review	Secure disposal – must be shredded
--	-----	---	------------------------------------

Pupil Attendance			
Type of file	Personal Information	Retention period	Action taken after retention period ends
Attendance registers	Yes	Every entry in the attendance register must be preserved for a period of 3 years after the date on which the last entry was made	Secure disposal
Correspondence relating to any absence (authorised or unauthorised)	Yes	Current academic year, + two years	Secure disposal

Special Educational Needs			
Type of file	Personal Information	Retention period	Action taken after retention period ends
SEND files, reviews and individual Education Health & Care Plans. Including advice and information provided to parents regarding educational needs and accessibility strategy	Yes	DOB of the pupil + 25 years	Secure disposal

9. Curriculum management and Extra-curricular Activities

Statistics and Management Information			
Type of file	Personal Information	Retention period	Action taken after retention period ends
Curriculum returns	Possibly	Current year + 3 years	Secure disposal

SATs results	Yes	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 of the whole year's SATs results. These could be kept for current year + 6 years to allow suitable comparison	Secure disposal
SATS Examination papers	Yes	The examination papers should be kept until any appeals/validation process is complete	Secure disposal
Published Admission Number (PAN) reports	No	Current year + 6 years	Secure disposal
Valued added and contextual data	No	Current year + 6 years	Secure disposal
Self-evaluation forms	No	Current academic year + 6 years	Secure disposal
Self-evaluation forms - external moderation	Yes	Until superseded	Secure disposal

Implementation of the Curriculum			
Type of file	Personal Information	Retention period	Action taken after retention period ends
Schemes of work	No	Current year + 1 year	Secure disposal
Timetable	No	Current year + 1 year	Secure disposal

Class record books	Yes	Current year + 1 year	Secure disposal
Mark books	Yes	Current year + 1 year	Secure disposal
Record of homework set	No	Current year + 1 year	Secure disposal
Pupils' work	Possibly	Where possible, the pupil's 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

School Trips			
Type of file	Personal Information	Retention period	Action taken after retention period ends
Parental consent forms for school trips where no major incident occurred	Yes	Until the conclusion of the trip	Secure disposal
Parental consent forms for school trips where a major incident occurred	Yes	Date of birth 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

Organisations and Groups that support the school			
Type of file	Personal Information	Retention period	Action taken after retention period ends

Parental consent forms for school trips where no major incident occurred	Yes	Until the conclusion of the trip	Secure disposal
Day books	Yes	Current year + 1 year	Secure disposal
Reports for outside agencies where the report has been included on the case file created by the outside agency	Yes	Current year + 1 year	Secure disposal
Referral forms	Yes	Current year + 1 year	Secure disposal
Mark books	Yes	Current year + 1 year	Secure disposal
Contact data sheets	Yes	Current then review, if no longer necessary or if superseded by new details	Secure disposal
Contact database entries	Yes	Current then review, if no longer necessary or if superseded by new details	Secure disposal
Group registers	Yes	Current year + 2 years	Secure disposal
Records relating to the creation and management of the PTA	Yes	Current Year + 6 Years.	Secure disposal

10. Retention of staff records

- a. The table below outlines the school's retention period of staff records and the action that will be taken after the retention period, in line with any requirements.
- b. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Personal Information	Retention period	Action taken after retention period ends
Operational			
Staff personnel file	Yes	Termination of Employment + 6 years, unless the member of staff is part of any case which falls under the terms of reference of IICSA. If this is the case, then the file will need to be retained until IICSA enquiries are completed.	Secure disposal
Annual appraisal /assessment records	Yes	Current year + 3 years	Secure disposal
Staff training – where the training leads to continuing professional development	Yes	Length of time required by the professional body	Secure disposal
Staff training – except where dealing with children, e.g. first aid or health and safety	Yes	This should be retained on the personnel file	Secure disposal
Staff training – where the training relates to children (e.g. safeguarding or other child related training)	Yes	Date of the training + 40 years (This retention period reflects that the IICSA may wish to see training records as part of an investigation)	Secure disposal
Sickness absence monitoring	Yes	If sickness pay is paid – Current Year + 3 Years. If sickness pay is not paid – current year + 3 years.	Secure disposal

Recruitment			
Records relating to the appointment of a new CEO/CFO/Headteacher	Yes	Unsuccessful attempts - date of appointment + 6 months. Successful attempts - add to personnel file and retain until end of appointment + 6 years, except in cases of negligence or claims of child abuse then at least 15 years.	Secure disposal
Records of unsuccessful job applicants	Yes	Date of appointment of successful candidate + 6 months	Secure disposal
Records of successful job applicants – Pre-employment vetting information + DBS Checks	Yes	Application forms, references and other documents – for the duration of the employee's employment + 6 years. You are not required to retain a copy of the DBS Certificate. If you wish to do so this should be kept for no longer than 6 months.	Secure disposal
Records of successful job applicants - Forms of proof of identity collected as part of the process of checking "portable" enhanced DBS disclosure	Yes	Where possible this process should be carried out using the on-line system. If it is necessary to take a copy of	Reviewed and a note kept of what was seen and what has been checked – if it is necessary to keep a copy this will be placed on the staff member's personal file, if not, Secure disposal

		documentation, then it should be retained on the staff personal file.	N.B. Financial auditor request copies of I.D.
Records of successful job applicants - Pre-employment vetting information – Evidence proving the right to work in the United Kingdom – successful candidates	Yes	Added to staff personnel file or, if kept separately, termination of employment, + not less than two years	Secure disposal
Disciplinary and grievance procedures			
Records relating to any allegation of a child protection nature against a member of staff	Yes	Added to staff personal file, and until the individual's normal retirement age, or 10 years from the date of the allegation – whichever is longer If allegations are malicious, they are removed from personal files If the allegations are found, they should be kept on the individual's personnel file and a copy provided to the person concerned. If the member of staff is part of any case which falls under the terms of reference of	Review & Secure disposal

		IICSA, then the file will need to be retained until IICSA enquiries are completed	
Oral warnings	Yes	Date of warning + 6 months	Secure disposal
Written warning – level 1	Yes	Date of warning + 6 months	Secure disposal
Written warning – level 2	Yes	Date of warning + 12 months	Secure disposal
Final warning	Yes	Date of warning + 18 months	Secure disposal
Records relating to unproven incidents	Yes	Conclusion of the case, unless the incident is child protection related and is disposed of as above	Secure disposal

11. Retention of senior leadership and management records

- a. The table below outlines the school's retention periods for senior leadership and management records, and the action that will be taken after the retention period, in line with any requirements.

Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Personal Information	Retention period	Action taken after retention period ends
Governance Records (Inc. Members, Trust Board, Committees & LGB's)			
Annual meeting schedule	No	Current year	Standard disposal
Agendas for relevant governance board meetings	No	Only if printed – Trust retains electronic Governance system	Secure disposal
Original, signed copies of the minutes of relevant governance board meetings, including attendance	Yes	10 years. Only if printed – Trust retains electronic Governance system	Secure disposal
Records relating to Governor Monitoring Visits	Possibly	Date of the visit + 3 years	Secure disposal
Reports presented to the relevant governance board	Possibly	Minimum of 10 years. Trust retains electronic Governance system	Secure disposal
Instruments of government, including articles of association	No	For the life of the school	Consult local authority archives before disposal
Action plans created and administered by the relevant governance board		Duration of the action plan + 3 years	Secure disposal
Policy documents created and administered by the relevant governance board		Until superseded	
Records relating to complaints dealt with by the relevant governance board	Yes	Major complaints: current year + 6 years. If negligence involved, then: current year + 15 years. If child protection or safeguarding issues are involved then: current year + 40 years	Secure disposal
Annual reports required by the DfE	Possibly	Date of report, + 10 years	Secure disposal

Proposals concerning changing the status of the school e.g. academy status, MAT, PAN	No	For the life of the organisation	Secure disposal
Records relating to the appointment of the Governance Professional/Clerk	Yes	Date on which clerk appointment ceases + 6 years	Secure disposal
Records relating to the terms of office of serving governance members, including evidence of appointment, DBS, disqualification checks etc	Yes	Date appointment ceases + 6 years	Secure disposal
Records relating to the election of parent and staff governors	Yes	Date of election + 6 months	Secure disposal
Records relating to appointments of governors, Trustees and members	Yes	Provided that the decision has been recorded in the minutes, the records relating to the appointment can be destroyed once the co-opted governor has finished their term of office (except where there have been allegations concerning children). In this case retain for 25 years	Secure disposal
Records relating to the election of Chair & Vice Chair	Yes	Once the decision has been recorded in the minutes, the records relating to the election can be destroyed	Secure disposal
Register of business interest	Yes	Date appointment ceases + 6 years (report on Trust websites for 12 months from date appointment ceases)	Secure disposal
Governance code of conduct	No	This is expected to be a dynamic document; one copy of each version should be kept for the life of the organisation	Secure disposal

Records relating to the training required and received by governors	No	Date appointment ceases + 6 years	Secure disposal
Records relating to the induction programme for new governors	No	Date appointment ceases + 6 years	Secure disposal
Scheme of delegation and terms of reference for committees	No	Until superseded or whilst relevant	Standard disposal
CEO/Head and senior leadership team (SLT)			
Minutes of SLT meetings and the meetings of other internal administrative bodies	Possibly	Date of the meeting + 3 years	Reviewed and Secure disposal
Reports created by SLT	Possibly	Date of the report + a minimum of 3 years	Reviewed and Secure disposal
Records created by SLT or members of staff with administrative responsibilities	Possibly	Current academic year + 3 years	Reviewed and Secure disposal
Correspondence created by SLT or members of staff with administrative responsibilities	Possibly	Date of correspondence + 3 years	Reviewed and Secure disposal
Professional development plan	Possibly	These should be held on the individual's personnel record. If not, then termination of employment + 6 years	Secure disposal
School development plan	No	Duration of the plan + 3 years	Secure disposal

12. Retention of health and safety records

- The table below outlines the school's retention periods for health and safety records, and the action that will be taken after the retention period, in line with any requirements.
- Electronic copies of any information and files will be destroyed in line with the retention periods below.
-

Type of file	Personal Information	Retention period	Action taken after retention period ends
Health and Safety			
Health and safety policy statements	No	Life of policy + 3 years	Standard disposal
Health and safety risk assessments	No	Life of risk assessment + 3 years provided that a copy of the risk assessment is stored with the accident report if an incident has occurred	Secure disposal
Accident reporting records relating to individuals who are over 18 years of age at the time of the incident	Yes	Accident records must be kept for 3 years	Secure disposal
Accident reporting records relating to individuals who are under 18 years of age at the time of the incident	Yes	Accident records must be kept for 3 years	Secure disposal
Records relating to any reportable death, injury, disease or dangerous occurrence (RIDDOR).	Yes	Date of incident + 3 years provided that all records relating to the incident are held on personnel file	Secure disposal
Control of Substances Hazardous to Health (COSHH)	Possibly	Date of incident + 6 years	Secure disposal
Process of monitoring of areas where employees and persons are likely to have come into contact with asbestos	No	Last action + 40 years	Secure disposal
Fire precautions logs	No	Current year + 6 years	Secure disposal
Health and safety records to show current state of building, including all alterations (wiring, plumbing, building works, etc.), to be passed on in the case of change of ownership	No	Pass to new owner on sale or transfer of building	

13. Retention of financial records

- The table below outlines the school's retention periods for financial records and the action that will be taken after the retention period, in line with any requirements.
- Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Personal Information	Retention period	Action taken after retention period ends
Payroll and pensions			
Absence/Sickness record	Yes	Current year + 3 years	Secure disposal
Payroll reports	Yes	Current year + 6 years	Secure disposal
Payslips	Yes	Current year + 6 years	Secure disposal
Mileage claims	Yes	Current year + 3 years	Secure disposal
Overtime claims	Yes	Current year + 3 years	Secure disposal
Maternity payments	Yes	Current year + 3 years	Secure disposal
Personal bank details	Yes	Until superseded + 3 years	Secure disposal
Elements e.g. pension rates, N.I. rates	No	Current year + 6 years	Secure disposal
Tax forms P6/P11/ P11D/P35/P45/P46/P48/P60	Yes	Current year + 6 years	Secure disposal
Pay awards	Yes	Current year + 6 years	Secure disposal
Risk management and insurance			
Employer's liability insurance certificate	No	Closure of the school + 40 years	Secure disposal – To be passed to LA if the school closes

Asset management			
Inventories of furniture and equipment	No	Current academic year + 6 years	Secure disposal
Burglary, theft and vandalism report forms	No	Current academic year + 6 years	Secure disposal
Accounts and statements including budget management			
Annual accounts	No	Current academic year + 6 years	Disposed of against common standards
Loans and grants managed by the Trust	No	Date of last payment + 12 years then review	Secure disposal
All records relating to the creation and management of budgets	No	Duration of the budget + 3 years	Secure disposal
Invoices, receipts, orders, requisitions and delivery notices	No	Current financial year + 6 years	Secure disposal
Records relating to the collection and banking of monies – if applicable	No	Current financial year + 6 years	Secure disposal
Records relating to the identification and collection of debt	No	Final payment of debt + 6 years	Secure disposal
Financial returns to the DfE and subsidiaries	No	Current academic year + 6 years	Disposed of against common standards
Pupil premium fund records	Yes	Date pupil leaves the provision + 6 years	Secure disposal
Contract management			
All records relating to the management of contracts under seal	No	Last payment on the contract + 12 years	Secure disposal
All records relating to the management of contracts under signature	No	Life of contract + 6 or 6 years or end of contract	Secure disposal
All records relating to the monitoring of contracts	No	End of contract or until the final payment has been made whichever is the longer	Secure disposal

School meals			
Free school meals registers	Yes	Current academic year + 3 years	Secure disposal
School meals registers	Yes	Current academic year + 3 years	Secure disposal
School meals summary sheets	Yes	Current academic year + 6 years	Secure disposal

14. Retention of other school records

- The table below outlines the school's retention periods for any other records held by the school, and the action that will be taken after the retention period, in line with any requirements.
- Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Personal Information	Retention period	Action taken after retention period ends
Property management			
Title deeds of properties belonging to the Trust	No	These should be retained permanently by the property's owner unless the property has been registered with the Land Registry	Transferred to new owners if the building is leased or sold
Plans of property belonging to the Trust	No	For as long as the building belongs to the Trust	Transferred to new owners if the building is leased or sold
Leases of property leased by or to the Trust	No	Expiry of lease + 6 years	Secure disposal
Records relating to the letting of Trust premises	No	Current financial year + 6 years	Secure disposal
Maintenance			
All records relating to the maintenance of the school carried out by contractors	No	These should be retained whilst the building belongs to the	Secure disposal

		school and should be passed on to any new owners if the building is leased or sold.	
All records relating to the maintenance of the school carried out by school employees including maintenance logs	No	These should be retained whilst the building belongs to the school and should be passed on to any new owners if the building is leased or sold.	Secure disposal
Government & LA Returns			
Secondary Transfer Sheets (primary)	Yes	Current year + 2 years	Secure disposal
Attendance returns	Yes	Current year + 1 year	Secure disposal
School census returns	Yes	Current year + 5 years	Secure disposal
OFSTED reports and papers where physical copy is held	No	Life of the report then review	Secure disposal
Operational administration			
Records relating to the creation and distribution of circulars to staff, parents or pupils	Possibly	Current academic year + 1 year	Standard disposal
School Privacy Notice which is sent to parents as part of GDPR compliance	No	Until superseded + 6 years	Standard disposal
Consents relating to school activities as part of GDPR compliance (for example, consent for use of images)	Yes	Consent will last whilst the pupil attends the school, it can therefore be destroyed when the pupil leaves	Secure disposal
Newsletters and other items with short operational use	Yes	Current academic year + 1 year	Standard disposal
Visitors' books and signing-in sheets	Possibly	Current academic year + 1 year	Reviewed then Secure disposal

15. Storing and protecting information

- The **DPO** will undertake a risk analysis to identify which records are vital to school management and these records will be stored in the most secure manner.
- The **DPO** will conduct a back-up of information on a **termly** basis to ensure that all data can still be accessed in the event of a security breach, e.g. a virus, and prevent any loss or theft of data.
- Where possible, backed-up information will be stored off the school premises, using a central back-up service operated by the Trust.
- Confidential paper records are kept in a locked filing cabinet, drawer or safe, with restricted access.
- Confidential paper records are not left unattended or in clear view when held in a location with general access.
- Digital data is coded, encrypted or password-protected, on a cloud network drive that is regularly backed-up.
- Where data is saved on removable storage or a portable device, the device is kept in a locked and fireproof filing cabinet, drawer or safe when not in use.
- Memory sticks are not used to hold personal information unless they are password-protected and fully encrypted.
- All electronic devices are password-protected to protect the information on the device in case of theft.
- Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.
- Staff and governors do not use their personal laptops or computers for school purposes.
- All members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.
- Emails containing sensitive or confidential information are password-protected to ensure that only the recipient is able to access the information. The password will be shared with the recipient in a separate email.
- Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- Where personal information that could be considered private or confidential is taken off the premises, to fulfil the purpose of the data in line with the GDPR, either in an electronic or paper format, staff take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.

Before sharing data, staff always ensure that:

- They have consent from data subjects to share it.

- Adequate security is in place to protect it.
- The data recipient has been outlined in a privacy notice.
- All staff members will implement a 'clear desk policy' to avoid unauthorised access to physical records containing sensitive or personal information. All confidential information will be stored in a securely locked filing cabinet, drawer or safe with restricted access.
- Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times.
- The physical security of the school's buildings and storage systems, and access to them, is reviewed **termly** by the **site staff** in conjunction with the **DPO**. If an increased risk in vandalism, burglary or theft is identified, this will be reported to the **CEO** and extra measures to secure data storage will be put in place.
- The Trust and individual schools take their duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.
- The **DPO** is responsible for continuity and recovery measures are in place to ensure the security of protected data.
- Any damage to or theft of data will be managed in accordance with the school's **Security Breach Management Plan**.

16. Accessing information

- **Prime7** is transparent with data subjects, the information we hold and how it can be accessed.
- All members of staff, parents of registered pupils and other users of the school, e.g. visitors and third-party clubs, are entitled to:
 - Know what information the school holds and processes about them or their child and why.
 - Understand how to gain access to it.
 - Understand how to provide and withdraw consent to information being held.
 - Understand what the school is doing to comply with its obligations under the GDPR.
- All members of staff, parents of registered pupils and other users of the school and its facilities have the right, under the GDPR, to access certain personal data being held about them or their child.
- Personal information can be shared with pupils once they are considered to be at an appropriate age and responsible for their own affairs; although, this information can still be shared with parents.
- Pupils who are considered to be at an appropriate age to make decisions for themselves are entitled to have their personal information handled in accordance with their rights.
- The school will adhere to the provisions outlined in the school's **GDPR Data Protection Policy** when responding to requests seeking access to personal information.

17. Digital continuity statement

- Digital data that is retained for longer than 6 years will be named as part of a **digital continuity statement**.
- The **DPO** will identify any digital data that will need to be named as part of a digital continuity statement.
- The data will be archived to dedicated files on the cloud servers, which are password-protected – this will be backed-up.
- Memory sticks will never be used to store digital data, subject to a digital continuity statement.

The following information will be included within the digital continuity statement:

- A statement of purpose and requirements for keeping the records
- The names of the individuals responsible for long term data preservation
- A description of the information assets to be covered by the digital preservation statement
- A description of when the record needs to be captured into the approved file formats
- A description of the appropriate supported file formats for long-term preservation
- A description of the retention of all software specification information and licence information
- A description of how access to the information asset register is to be managed in accordance with the GDPR

18. Information audit

- The school conducts information audits on an **annual** basis against all information held by the school to evaluate the information the school is holding, receiving and using, and to ensure that this is correctly managed in accordance with the GDPR. This includes the following information:
 - Paper documents and records
 - Electronic documents and records
 - Databases
 - Sound recordings
 - Video and photographic records
 - Hybrid files, containing both paper and electronic information

- The information audit may be completed in a number of ways, including, but not limited to:
 - Interviews with staff members with key responsibilities – to identify information and information flows, etc.
 - Questionnaires to key staff members to identify information and information flows, etc.
 - A mixture of the above
- The **DPO** is responsible for completing the information audit. The information audit will include the following:
 - The school's data needs
 - The information needed to meet those needs
 - The format in which data is stored
 - How long data needs to be kept for
 - Vital records status and any protective marking
 - Who is responsible for maintaining the original document
- The DPO will consult with staff members involved in the information audit process to ensure that the information is accurate.
- Once it has been confirmed that the information is accurate, the **DPO** will record all details on the school's **Information Asset Register**.
- The information displayed on the **Information Asset Register** will be shared with the **CEO** to gain their approval.

19. Disposal of data

- Where disposal of information is outlined as standard disposal, this will be recycled appropriate to the form of the information, e.g. paper recycling, electronic recycling.
- Where disposal of information is outlined as secure disposal, this will be shredded or pulped and electronic information will be scrubbed clean and, where possible, cut. The **DPO** will keep a record of all files that have been destroyed.
- Where the disposal action is indicated as reviewed before it is disposed, the **DPO** will review the information against its administrative value – if the information should be kept for administrative value, and the **DPO** will keep a record of this.
- If, after the review, it is determined that the data should be disposed of, it will be destroyed in accordance with the disposal action outlined in this policy.

- Where information has been kept for administrative purposes, the **DPO** will review the information again after 3 years and conduct the same process. If it needs to be destroyed, it will be destroyed in accordance with the disposal action outlined in this policy. If any information is kept, the information will be reviewed every **3** subsequent years.
- Where information must be kept permanently, this information is exempt from the normal review procedures

20. Monitoring and review

- This policy will be reviewed on an **annual** basis by the **DPO** in conjunction with the **CEO**.
- Any changes made to this policy will be communicated to all members of staff and the governance boards.