Beaminster School

Data Protection Policy (Draft)

Date agreed by the Resources Committee:
Date adopted by Governing Body:
Date to be reviewed: April 2022
(Review cycle 3 years, unless significant legal changes)

CONTENTS

1. Statement of intent
   - 1.6 Other related policies

2. Record retention and processing policy
   - 2.1 Document Storage
   - 2.2 Computer Security
   - 2.3 Retention of Data
   - 2.4 Document Destruction
   - 2.5 Access to Personal Data
   - 2.6 Pupils
   - 2.7 Staff (including peripatetic staff where relevant)
   - 2.8 School Governors
   - 2.9 Parents
   - 2.10 Volunteers

3. Roles and responsibilities
   - 3.1 Data Protection Officer
   - 3.2 Data Controller
   - 3.3 Principal Data Processor

4. Home working

5. Appendices
   - 5.1 Data Breach Guidance
   - 5.2 Types of security breach and causes
   - 5.3 Secure Configuration
   - 5.4 Network Security
   - 5.5 Malware Prevention
   - 5.6 Removable media controls

Annex: DfE Annual review of school records and safe data destruction checklist

1. STATEMENT OF INTENT

This is a statement of Data Protection Policy (**the Policy"**) adopted by Beaminster School (**the "School"**) in June 2019.

1.1 The School keeps personal data on Pupils, Parents, Staff, Governors and Volunteers as set out below. This Policy describes how that data, whether held electronically or on paper, is handled and stored having regard to the requirements of the Data Protection Act 2018.

1.2 This Policy helps to ensure the confidentiality of personal data supplied to the School and to protect the School from reputational damage if that information were to be accessed without proper authorisation.

1.3 All of us have a responsibility for ensuring that personal data is collected, stored and handled appropriately in accordance with this Policy.

1.4 The School endorses fully the Data Protection Principles as detailed in Schedule 1 of the Data Protection Act 2018 and will, through strict application of criteria and controls ensure compliance. Specifically, the Principles require that personal information will:

- be processed fairly and lawfully;
- only be used for specified and lawful purposes and shall not be used in any manner incompatible with those purposes;
- be adequate, relevant and not excessive;
- be accurate and, where necessary, kept up to date;
- not be kept any longer than is necessary;
- be used in accordance with the rights of the individuals to whom it relates;
- be protected against unauthorised use, theft, accidental loss, destruction or damage by the use of appropriate technical and organisational measures;
- not be transferred to a country or territory which does not have an adequate level of legal protection for the rights of individuals in relation to the processing of their personal data.

1.5 The School also fully endorses the Individuals' Rights as detailed in the General Data Protection Legislation. Specifically, this grants individuals the following rights:

- the right to be informed (fair processing of information, privacy notices, transparency);
- the right of access (confirmation/access to personal data);
- the right to rectification (must respond within 30 days);
- the right to erasure (can request deletion (certain circumstances));
- the right to restrict processing (may store data but not process it);
- the right to data portability (individuals may obtain/reuse their data across different services);
- the right to object (profiling; direct marketing; scientific/historical research and statistics);
- rights in relation to automated decision making and profiling (significant effect without human intervention).

1.6 Other related policies for reference:
- Acceptable use of IT Policy
- E-Safety Policy
- Data Breach protocol
- Social Networking Policy

2 RECORD RETENTION AND PROCESSING POLICY

2.1 Document Storage

Paper documents are held in lockable metal filing cabinets in the School Office for as long as they are needed.

2.2 Computer Security

Data on our Servers is password protected but not encrypted. All data is backed up in a different building on a separate server. Only the Data Controller and Principal Data Processor have access to this server.

Encryption is not a panacea: in the event of a problem with the computer system it makes the recovery process or resolving simple problems more complicated and increases the risk of us being unable to access and restore our files. Even if those files were encrypted if someone manages to crack a user's password they would be able to access all the data because it would be automatically decrypted. Encryption would be of benefit if someone were to physically steal our Server because the thief can't simply plug it in to another Server to read the files (any reset 'tools' would detect interference and prevent decryption). That apart the risk of such a theft is considered to be very low.

Servers connected to the Internet, as ours is, are always at a small risk of being hacked and this can't be entirely removed, only reduced and the best way to do that is with strong passwords that are regularly changed. The Admin server is configured to enforce the requirement for a strong password which has to be changed half termly.

2.3 Retention of Data

The period of retention, the means of storage and the processes for data manipulation and for ultimate destruction vary according to the purpose for which the data are used as described in the DfE 'School records and safe data destruction checklist'. This document is annexed and is reviewed annually.

2.4 Document Destruction

Paper documents that are beyond their retention date will be destroyed by means of shredding, or removed and disposed through our confidential waste disposal.

2.5 Access to Personal data

All individuals on whom we hold data are entitled to:

i. Ask what information we hold on them and why
ii. Ask how to gain access to it
iii. Be informed how to keep it up to date
iv. Be informed by us as to how we are meeting our data protection obligations

Individuals wishing to access their personal data for any of the purposes detailed in the General Data Protection Legislation should contact the Head Teacher who is the School's Data Controller (See Section 3.2).

2.6 Pupils

The categories of pupil information that we process include**:**

- Personal identifiers and contacts (such as name, unique pupil number, contact details and address)
  Characteristics (such as ethnicity, language, and free school meal eligibility)
- Safeguarding information (such as court orders and professional involvement)
  Special educational needs (including the needs and ranking)
- Medical and administration (such as doctors information, child health, dental health, allergies, medication and dietary requirements)
- Attendance (such as sessions attended, number of absences, absence reasons and any previous schools attended)
- Assessment and attainment (such as Key Stage 2, 3, 4 or 5 results)
- Behavioral information (such as exclusions and any relevant alternative provision put in place)

We collect and use pupil information, for the following purposes:

- To support pupil learning
- To monitor and report on pupil attainment progress
- To provide appropriate pastoral care
- To assess the quality of our services
- To keep children safe (food allergies, or emergency contact details)
- To meet the statutory duties placed upon us for DfE data collections

2.7 Staff (including peripatetic staff where relevant)

The categories of staff information that we collect and process include:

- Personal information (such as name, employee or teacher number, national insurance number)
- Characteristics information (such as gender, age, ethnic group)
- Contract information (such as start date, hours worked, post, roles and salary information)
- Work absence information (such as number of absences and reasons)
- Qualifications (and, where relevant, subjects taught).
-

We collect and use staff information to:

- Enable the development of a comprehensive picture of the workforce and how it is deployed
- Inform the development of recruitment and retention policies
- Enable individuals to be paid

We hold data securely for the set amount of time shown in our data retention schedule.

2.8 School Governors

The categories of School Governor information that we collect and process include:

- Personal identifiers, contacts and characteristics (such as name, date of birth, contact details, e-mail address and postcode)
- Governance details (such as role, start and end dates)
- Skills and business interests

We collect and use School Governor information, for the following purposes:

- To meet the statutory duties placed upon us
- To promulgate details of Meetings (Agendas and supporting papers) and Minutes of Meetings held.

We hold data securely for the set amount of time shown in our data retention schedule.

2.9 Parents

The categories of parent information that we collect and process include:

- Names, address and contact details (e-mail, telephone and post code)

We collect and use parent information for the following purposes:

- Contacting the parent in the event of an illness, accident or emergency involving their child
- Promulgating information on curricular and extra curricular activities involving or potentially involving their child
- Distribution of Newsletters and Circulars covering general School activities.

We hold data securely for the set amount of time shown in our data retention schedule.

2.10 Volunteers

The School maintains paper and computer records of volunteers who come in to assist with various activities such as reading with pupils, breakfast clubs etc. The personal data we hold are their name, address, telephone number, and e-mail address and are used solely to contact them if there is a need to do so. Records are updated as information is supplied by the volunteer and are deleted when the volunteering ceases.

3. ROLES AND RESPONSIBILITIES

3.1 Data Protection Officer (DPO): The Data Protection Officer is a School Governor and is responsible for:

- Advising school leadership and staff about their data obligations, monitoring compliance, including managing internal data protection activities, ensuring relevant training, and conducting internal audits

- Implementing effective strategies for the management of risks posed by Internet use, and to keep its network services, data and users secure.

3.2 **Data Controller:** The data controller is the Head Teacher and is responsible for the overall monitoring and management of data security, alongside the Senior IT Technician.

3.3 Principal Data Processor: The Principal Data Processor is the School Administrator who is responsible to the Data Controller for all data storage and processing on a day-to-day basis.

4. HOME WORKING

The School understands that staff may need to access pupil assessment records from areas other than on the premises. Effective security management has been established to prevent access to, or leakage of, data, as well as any possible risk of malware.

The data controller will end to end encrypt all school-owned devices for personal use, such as laptops, mobile phones and tablets, to ensure that they are password protected. If any portable devices are lost, this will prevent unauthorised access to personal data.

In accordance with the Equality Duty we seek to ensure that all pupils achieve their best, according to their capabilities and regardless of their special needs, disability, gender, race, culture, social, economic, ethnic, religious background and denominational diversity.

Beaminster School recognises that the welfare of the child is paramount and takes seriously its responsibility to safeguard and promote the welfare of the children and young people in its care.

APPENDICES

5.1 Data Breach Guidance

Any individual that discovers a security data breach will report this immediately to the Headteacher and data controller. When an incident is raised, the Data Protection Officer will record the following information via the template provided:

- Name of the individual who has raised the incident
- Description of the incident
- Description of any perceived impact
- Description & identification codes of any devices involved, e.g. School-owned laptop
- Location of the equipment involved
- Contact details for the individual who discovered the incident

The school's Data Protection Officer will take the lead in investigating the breach, supported by the Headteacher, and will be allocated the appropriate time and resources to conduct this. The Data Protection Officer, as quickly as reasonably possible, will ascertain the severity of the breach and determine if any personal data is involved or compromised. The Data Protection Officer will oversee a full investigation and produce a comprehensive report. The cause of the breach, and whether or not it has been contained, will be identified – ensuring that the possibility of further loss/jeopardising of data is eliminated or restricted as much as possible. If the Data Protection Officer determines that the severity of the security breach is low, the incident will be managed in accordance with the following procedures:

- In the event of an internal breach, the incident is recorded using an incident log, and by identifying the user and the website or service they were trying to access.
- The Headteacher will review responsibility and take any necessary actions in accordance with the processes outlined in the E-Safety, or other, Policies..
- The data controller and Senior IT Technician will work with the third-party provider to provide an appropriate response to the attack, including any in-house changes.

Any further action which could be taken to recover lost or damaged data will be identified – this includes the physical recovery of data, as well as the use of back-ups.
Where the security risk is high, the school will establish what steps need to be taken to prevent further data loss which will require support from various school departments and staff. This action will include:

- Informing relevant staff of their roles and responsibilities in areas of the containment process.
- Taking systems offline.
- Retrieving any lost, stolen or otherwise unaccounted for data.
- Restricting access to systems entirely or to a small group.
- Backing up all existing data and storing it in a safe location.
- Reviewing basic security, including:
- Changing passwords and login details on electronic equipment.
- Ensuring access to places where electronic or hard data is kept is monitored and requires authorisation.

Where appropriate, e.g. if offences have been committed under the Computer Misuse Act 1990, the Data Protection Officer will inform the police of the security breach.
The data controller will test all systems to ensure they are functioning normally, and the incident will only be deemed 'resolved' when it has been assured that the school's systems are safe to use.

5.2 Types of security breach and causes

Unauthorised use without damage to data – involves unauthorised persons accessing data on the school system, e.g. 'hackers', who may read the data or copy it, but who do not actually damage the data in terms of altering or deleting it.

Unauthorised removal of data – involves an authorised person accessing data, who removes the data to pass it on to another person who is not authorised to view it, e.g. a staff member with authorised access who passes the data on to a friend without authorised access – this is also known as data theft. The data may be forwarded or deleted altogether.

Damage to physical systems – involves damage to the hardware in the school's ICT system, which may result in data being inaccessible to the school and/or becoming accessible to unauthorised persons.

Unauthorised damage to data – involves an unauthorised person causing damage to data, either by altering or deleting it. Data may also be damaged by a virus attack, rather than a specific individual.

Breaches in security may be caused as a result of actions by individuals, which may be accidental, malicious or the result of negligence – these can include:

- Accidental breaches, e.g. as a result of insufficient training for staff, so they are unaware of the procedures to follow.
- Malicious breaches, e.g. as a result of a hacker wishing to cause damage to the school through accessing and altering, sharing or removing data.
- Negligence, e.g. as a result of an employee that is aware of school policies and procedures, but disregards these.

Breaches in security may also be caused as a result of system issues, which could involve incorrect installation, configuration problems or an operational error – these can include:

- Incorrect installation of anti-virus software and/or use of software which is not the most up-to-date version, meaning the school software is more vulnerable to a virus
- Incorrect firewall settings are applied, e.g. access to the school network, meaning individuals other than those required could access the system
- Confusion between backup copies of data, meaning the most recent data could be overwritten

5.3 Secure configuration

An inventory will be kept of all IT hardware and software currently in use at the school, including mobile phones and other personal devices provided by the school. This will be stored in the finance office and will be audited on an annual basis to ensure it is up-to-date.
Any changes to the IT hardware or software will be documented using the inventory, and will be authorised by the Data Protection Officer before use.

All systems will be audited on a termly basis to ensure the software is up-to- date. Any new versions of software or new security patches will be added to systems, ensuring that they do not affect network security, and will be recorded on the inventory.

5.4 Network Security

The school employs firewalls in order to prevent unauthorised access to the systems.
This is managed by the Senior IT Technician and updated regularly.

5.5 Malware prevention

The school understands that malware can be damaging for network security and may enter the network through a variety of means, such as email attachments, social media, malicious websites or removable media controls.

The school employs a number of protective systems, including ESET Endpoint Antivirus, that are updated regularly by the Senior IT Technician to secure malware protection.

Filtering of websites, particularly through the South West Grid system, will ensure that access to websites with known malware is blocked immediately and reported to the Data controller.

The school will use mail security technology, which will detect and block any malware that is transmitted by email. This will also detect any spam or other messages which are designed to exploit users. E.g. unusual email activity passes straight to junk

The Data controller will review the mail security technology on a termly basis to ensure it is kept up-to-date and effective.

5.6 Removable media controls

Pupils and staff are not permitted to use their personal devices where the school shall provide alternatives, such as work laptops, tablets and USB sticks, unless instructed otherwise by the Headteacher.

Staff who use school-owned laptops, tablets and other portable devices will use them for work purposes, whether on or off school premises. The data controller will use encryption to filter the use of websites on these devices, in order to prevent inappropriate use and external threats which may compromise network security when bringing the device back onto the premises..

All data will be held on systems centrally in order to reduce the need for the creation of multiple copies, and/or the need to transfer data using removable media controls.

The Wi-Fi networks at the school are password protected and will only be given out as required. A separate Wi-Fi network exists for staff, external agencies and sixth form pupils for their personal devices, such as mobile phones or tablets.

There is very limited need for external memory sticks, except for use in photography and media studies, where other methods are more effective data can be uploaded via email or office 365.

5.7 Backing up Data

A back-up of all electronic data held by the school occurs on a daily basis, and the date of the back-up is recorded using a log. Each back-up is retained for up to three months before being deleted. Back-ups are run overnight and are completed before the beginning of the next school day. Upon completion of back-ups, data is stored on the school’s hardware which is password protected.

Data is also replicated weekly and stored offsite on a Network Attached Storage device (encrypted drive). Only authorised personnel are able to access the school’s data.

5.8 Other

Staff, and students receive regular training on GDPR and the necessity for safeguarding data.

External Software providers (E.g. SIMS and ParentMail) are always checked to be compliant with GDPR regulations.

The sharing of electronic information (E.g. Government, Local Authority, other schools and colleges) is only undertaken where we have been assured they are independently compliant.

Data protection extends to the recording of written files and data printed from electronic files. All staff will minimise the need to do this and destroy sensitive information through our data destruction sacks. Any lost information should be reported directly to the Headteacher and dealt with in the same manner as under our Data Breach Protocol.

Annex: DfE Annual review of school records and safe data destruction checklist

Completion page

School name: _____

Review completed by: _____

Date: _____

Approved by Headteacher: _____

Date: _____

Note – The completion of this review should be shared at the Governors meeting and minuted.

A. Summary of areas reviewed:

Ref	Area	Pages	Annual Review Completed Tick (√)	Reviewer Initials
1	Management of the School	5 to 9		
2	Human Resources	10 to 12		
3	Financial Management of the School	13 to 14		
4	Property Management	15		
5	Pupil Management	16 to 17		
6	Curriculum Management	18		
7	Extra-Curricular Activities	19 to 20		
8	Central Government and Local Authority	21		
9	List of School Records and Data safely destroyed	22		

Contents

A. Aims 10
B. Safe Destruction of Data 10
(i) Disposal of records that have reached the end of the minimum retention period allocated 10
(ii) Safe destruction of records 11
(iii) Freedom of Information Act 2000 (FoIA 2000) 11
1. Management of the School 13
2. Human Resources 18
3. Financial Management of the School 21
4. Property Management 23
5. Pupil Management 24
6. Curriculum Management 26
7. Extra Curriculum Management 27
8. Central Government and Local Authority 29
Appendix A – List of School Records and Data safely destroyed 30

A. Aims

This checklist has been produced based on the "Information Management Toolkit for Schools" (IMTIS) dated 1 February 2016 and developed and published by the Information Record Management Society ("IRMS").

This checklist has been produced in accordance with the guidance produced by the DFE in April 2018 in the "GDPR Toolkit for Schools" and is in accordance with the Data Protection rules and Freedom of Information Act (2000) legislation.

This is a checklist developed to enable School Business Managers, Clerks, SENCO and other School Staff to carry out an efficient annual review and safe destruction of school records and information.

Where there is legal statute behind a requirement this is detailed in the IMTIS document.

B. Safe Destruction of Data

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

The fifth data protection principle as per the data protection rules (updated for GDPR) 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"

In each school, the leadership 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.

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

Whatever decisions are made they need to be documented as part of the records management policy within the school.

(ii) 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 of to a waste paper merchant or disposed of in other appropriate ways. Do not put records in with the regular waste or a skip unless there is no other alternative.

There are companies who can provide confidential waste bins and other services which can be purchased to ensure that records are disposed of in an appropriate way.

a) 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.

   The shredding needs to be planned with specific dates and all records should be identified as to the date of destruction.

   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.

b) Where records are destroyed internally, the process must ensure that all records are recorded are authorised to be destroyed by a member of the Leadership team and the destruction recorded. Records should be shredded as soon as the record has been documented as being destroyed.

(iii) 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 rules and the Freedom of Information Act 2000.

Version Control History
Second Edition – June 2019

1. Management of the School

This section contains retention periods connected to the general management of the school. This covers the work of the Governing Body, the Headteacher and the senior management team, the admissions process and operational administration.

1.1 Governing Body					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
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	If the school is unable to store these then they should be offered to the County Archives Service	
	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 relating to staff	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 permanently	SECURE DISPOSAL or retain with the signed set of the minutes	
1.1.4	Meeting papers relating to the annual parents' meeting held under section 33 of the Education Act 2002	No	Date of the meeting + a minimum of 6 years	SECURE DISPOSAL	

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 (continued…)					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
1.1.5	Instruments of Government including Articles of Association	No	PERMANENT	These should be retained in the school whilst the school is open and then offered to County Archives Service when the school closes.	
1.1.6	Trusts and Endowments managed by the Governing Body	No	PERMANENT	These should be retained in the school whilst the school is open and then offered to County Archives Service when the school closes.	
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 Body	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 disputes	SECURE DISPOSAL	
1.1.10	Annual Reports created under the requirements of the Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002	No	Date of report + 10 years	SECURE DISPOSAL	
1.1.11	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	

1.2 Head Teacher and Senior Management Team					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
1.2.1	Log books of activity in the school maintained by the Head Teacher	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	These could be of permanent historical value and should be offered to the County Archives Service if appropriate	
1.2.2	Minutes of Senior Management Team meetings and the meetings of other internal administrative bodies	There may be data protection issues if the minutes refers to individual pupils or members of staff	Date of the meeting + 3 years then review	SECURE DISPOSAL	
1.2.3	Reports created by the Head Teacher or the Management 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 head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	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 head teachers, deputy head teachers, heads of year 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	

1.3 Admissions Process					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
1.3.1	All records relating to the creation and implementation of the School Admissions' Policy	No	Life of the policy + 3 years then review	SECURE DISPOSAL	
1.3.2	Admissions – if the admission is successful	Yes	Date of admission + 1 year	SECURE DISPOSAL	
1.3.3	Admissions – if the appeal is unsuccessful	Yes	Resolution of case + 1 year	SECURE DISPOSAL	
1.3.4	Register of Admissions	Yes	Every entry in the admission register must be preserved for a period of three years after the date on which the entry was made.[3]	REVIEW Schools may wish to consider keeping the admission register permanently as often schools receive enquiries from past pupils to confirm the dates they attended the school.	
1.3.5	Admissions – Secondary Schools – Casual	Yes	Current year + 1 year	SECURE DISPOSAL	
1.3.6	Proofs of address supplied by parents as part of the admissions process	Yes	Current year + 1 year	SECURE DISPOSAL	
1.3.7	Supplementary Information form including additional information such as religion, medical conditions etc	Yes			
	For successful admissions		This information should be added to the pupil file	SECURE DISPOSAL	
	For unsuccessful admissions		Until appeals process completed	SECURE DISPOSAL	

1.4 Operational Administration					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
1.4.1	General file series	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	

2. Human Resources

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

2.1 Recruitment					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
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	
2.13	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	The school does not have to keep copies of DBS certificates. If the school does so the copy must NOT be retained for more than 6 months		
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		
2.1.6	Pre-employment vetting information – Evidence proving the right to work in the United Kingdom[4]	Yes	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		

2.2 Operational Staff Management					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
2.2.1	Staff Personal File	Yes	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					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
2.3.1	Allegation of a child protection nature against a member of staff including where the allegation is unfounded[5]	Yes	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	SECURE DISPOSAL [If warnings are placed on personal files then they must be weeded from the file]	
	written warning – level 1		Date of warning + 6 months		
	written warning – level 2		Date of warning + 12 months		
	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 case	SECURE DISPOSAL	

2.4 Health and Safety					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
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	Recordsrelatingto 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			
	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	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	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 log books	No	Current year + 6 years	SECURE DISPOSAL	

2.4 Payroll and Pensions					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
2.5.1	Maternity pay records	Yes	Current year + 3 years	SECURE DISPOSAL	
2.5.2	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	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					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
3.1.1	Employer's Liability Insurance Certificate	No	Closure of the school + 40 years	SECURE DISPOSAL	

3.2 Asset Management					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
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	

3.3 Accounts and Statements including Budget Management					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
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 ofmonies	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					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
3.4.1	All records relating to the management of contracts under seal	No	Last payment on the contract + 12 years	SECURE DISPOSAL	
3.4.2	All records relating to the management of contracts under signature	No	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					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
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					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
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					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
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					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
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 Safety above

5.1 Pupil's Educational Record					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
5.1.1	Pupil's Educational Record required by The Education (Pupil Information) (England) Regulations 2005	Yes			
	Primary		Retain whilst the child remains at the primary school	The file should follow the pupil when he/she leaves the primary school. [3]	
	Secondary		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		
5.1.3	Child Protection information held on pupil file		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		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	

[3] This will include: (i) to another primary school (ii) to a secondary school (iii) to a pupil referral unit (iv) If the pupil dies whilst at primary school the file should be returned to the Local Authority to be retained for the statutory retention period. If the pupil transfers to an independent school, transfers to home schooling or leaves the country the file should be returned to the Local Authority to 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. It makes more sense to transfer the record to the Local Authority as it is more likely that the pupil will request the record from the Local Authority

5.2 Attendance					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
5.2.1	Attendance Registers	Yes	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		Current academic year + 2 years	SECURE DISPOSAL	

5.3 Special Educational Needs					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
5.3.1	Special Educational Needs files, reviews and Individual Education Plans	Yes	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	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	
			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	
			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					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
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) Reports	Yes	Current year + 6 years	SECURE DISPOSAL	
6.1.4	Value Added and Contextual Data	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					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
6.2.1	Schemes of Work	No	Current year + 1 year	Review these records at the end of each year and allocate a further retention period or SECURE DISPOSAL	
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 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 Curriculum Management

7.1 Educational Visits outside the Classroom					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
7.1.1	Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Primary Schools	No	Date of visit + 14 years	SECURE DISPOSAL	
7.1.2	Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Secondary Schools	No	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	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	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		

7.2 Walking Bus					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
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 [If these records are retained electronically any back up copies should be destroyed at the same time]	

7.3 Family Liaison Officers and Home School Liaison Assistants					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
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

8.1 Local Authority					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
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	

8.2 Central Government					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
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	

Appendix A – List of School Records and Data safely destroyed

The following sheet can be completed or alternatively documented in a spreadsheet.

Ref Number	File/Record Title	Description	Reference or Cataloguing Information	Number of Files Destroyed	Method of destruction	Confirm (i) Safely destroyed (ii) In accordance with Data Retention Guidelines Tick (√)
e.g.	*School Invoices*	*Copies of purchase invoices dated 2011/12*	*Folders marked "Purchase Invoices 2011/12" 1 to 3*	*3 Folders*	*Shredding*	√
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						