



Governor Committee Responsible:	FGB	Staff Lead:	Acting Headteacher Michala Reid
Status	Statutory	Review Cycle	Annual / Biennial / Tri-annual
Ratified by	Tracey Johnson, Chair of Governors Michala Reid, Acting Headteacher	Ratification date	February 26
Next Review Date	February 27	To be read in conjunction with	• Privacy Notice • Complaints procedure • Consent form • CCTV • Freedom of Information Policy

Data Protection Policy

General Data Protection Regulation

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category (SC) and criminal offence (CO) data under certain specified conditions.

This document meets the requirement at paragraph 1 of Schedule 1 to the Data Protection Act 2018 that an appropriate policy document be in place where the processing of special category personal data is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment, social security or social protection.

It also meets the requirement at paragraph 5 of Schedule 1 to the Data Protection Act 2018 that an appropriate policy document be in place where the processing of special category personal data is necessary for reasons of substantial public interest. The specific conditions under which data may be processed for reasons of substantial public interest are set out at paragraphs 6 to 28 of Schedule 1 to the Data Protection Act 2018 and the School intends to rely on these as and when appropriate, with particular reliance on paragraph 18, 'Safeguarding of children and individuals at risk' and paragraph 17, 'Counselling'.

1. Introduction

In order to work effectively **Berry Hill Primary School** has to collect and use information about people with whom it works. This may include (past, present and future) pupils, parents, teachers, trustees, members of the public, contractors and suppliers. In addition, we may be required by law to collect and use information in order to comply with the requirements of central government.

All personal information must be handled and dealt with properly, regardless of how it is collected, recorded and used, and whether it is on paper, in computer records or recorded by other means. We are all responsible for its safe handling.

This document sets out the principles of data protection, our responsibilities, and the access rights of individuals, as well as information sharing and complaints.

2. Scope/ Our Commitment

This policy applies to all staff, governors, contractors, agents, representatives and temporary staff, working for or on behalf of the School. The requirements of this policy are mandatory for all of these parties.

Berry Hill Primary School regards the lawful and correct treatment of personal information as critical to its successful operation, maintaining confidence between the school and those it interacts with. The school will ensure that it treats personal information correctly in accordance with the law.

Berry Hill Primary School fully endorses and adheres to the principles of Data Protection as set out in the Data Protection Act (2018) and the General Data Protection Regulation (GDPR).

Berry Hill Primary School is committed to ensuring that their staff are aware of data protection policies, legal requirements and that adequate training is provided.

Changes to data protection legislation, under the GDPR and DPA, shall be monitored and implemented in order to remain compliant with all requirements.

3. Principles of Data Protection

The GDPR outlines seven key principles for anyone who processes personal data. These principles form the basis of our approach to processing personal data.

[Guide to data protection | ICO](#)

[Key definitions of the Data Protection Act | ICO](#)

- ensure that data is fairly and lawfully processed
- process data only for limited purposes
- ensure that all data processed is adequate, relevant and not excessive
- ensure that data processed is accurate
- ensure that data is not kept for longer than is necessary
- process the data in accordance with the data subject's rights
- ensure that data is secure
- ensure that data is not transferred to other countries without adequate protection.

4. Responsibilities

Berry Hill Primary School is registered as a data controller with the ICO and will renew this registration as required.

Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register.

[Register of data controllers | ICO](#)

Data breaches shall be notified within 72 hours to the individual(s) concerned and the ICO.

The members of staff responsible for data protection within the School are mainly School Business Manager, Headteacher and SLT. However, all staff must treat all pupil (or other relevant) information in a confidential manner and follow the guidelines set out in this document.

We have appointed Gloucestershire County Council as our Data Protection Officer. They can be contacted on 01452 583619 or schoolsdpo@gloucestershire.gov.uk

5. Definitions of Data

Personal data is information about living, identifiable individuals. It covers both facts and opinions about the individual but need not be sensitive information. The GDPR makes a distinction between personal data and "special category" (sensitive) data. Special category personal data requires stricter conditions for processing.

Personal data is Defined in s(1) of the GDPR, as 'data which relates to a living individual who can be identified from that data, or from that data and other information which is in the possession of, or is likely to come into the possession of the data controller' (the School is a data controller), and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other in respect of the individual.

Special Category Data is information about racial or ethnic origin, sexual life or sexual orientation, biometric and genetic data, religious beliefs (or similar), physical or mental health/condition, membership of a trade union, political opinions or beliefs, details of proceedings in connection with an offence or an alleged offence.

6. Processing Personal Data

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law. When special category personal data, criminal conviction data or data about offences, is processed, a lawful basis and additional condition will be satisfied.

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest**, and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by [The Data Protection, Privacy and Electronic Communications \(Amendments etc\) \(EU Exit\) Regulations 2020](#)
- [Data Protection Act 2018 \(DPA 2018\)](#)

It is based on guidance published by the Information Commissioner's Office (ICO) on the [UK GDPR](#). It meets the requirements of the [Protection of Freedoms Act 2012](#) when referring to our use of biometric data. It also reflects the ICO's [guidance](#) for the use of surveillance cameras and personal information. In addition, this policy complies with regulation 5 of the [Education \(Pupil Information\) \(England\) Regulations 2005](#), which gives parents the right of access to their child's educational record.

7. Fair Processing / Privacy Notice

We shall be transparent about the intended processing of all data including criminal offence data and communicate these intentions via notification to staff, parents and pupils prior to the processing of an individual's data.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as 'Children' under the legislation.

8. Sharing Data

There may be circumstances where the school is required either by law or in the best interests of our pupils or staff to pass information on to external authorities, for example local authorities, Ofsted, or the department of health.

These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

Any proposed change to the processing of an individual's data shall first be notified to them.

Personal data about pupils will not be disclosed to third parties without the consent of the child's parent or carer, unless it is obliged by law or in the best interest of the child. Data may be disclosed to the following third parties without consent:

- **Other schools**

If a pupil transfers from **Berry Hill Primary School** to another school, their records and other data that relates to their health and welfare will be forwarded on to the new school. This will support a smooth transition from one school to the next and ensure that the child is provided for as necessary. It will aid continuation which should ensure that there is minimal impact on the child's academic progress as a result of the move.

- **Examination authorities**

This may be for registration purposes, to allow the pupils at our school to sit examinations set by external exam bodies.

- **Health authorities**

As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.

- **Police and courts**

If a situation arises where a criminal investigation is being carried out, we may have to forward information on to the police to aid their investigation. We will pass information on to courts as and when it is ordered.

- **Social workers and support agencies**

In order to protect or maintain the welfare of our pupils, and in cases of suspected child abuse, it may be necessary to pass personal data on to social workers or support agencies.

- **Education division**

Schools may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.

Under no circumstances will the school disclose information or data:

- that would cause serious harm to the child's or anyone else's physical or mental health or condition
- indicating that the child is or has been subject to child abuse or may be at risk of it, where the disclosure would not be in the best interests of the child
- recorded by the pupil in an examination
- that would allow another person to be identified or identifies another person as the source, unless the person is an employee of the school or a local authority or has given consent, or it is reasonable in the circumstances to disclose the information without consent. The

exemption from disclosure does not apply if the information can be edited so that the person's name or identifying details are removed

- in the form of a reference given to another school or any other place of education and training, the child's potential employer, or any national body concerned with student admissions.

9. Photographs and Videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- Within school on notice boards and in school magazines, brochures, prospectuses newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns or third party benefactors (such as charities or companies who provide financial support to the school).
- Online on our school website or social media pages/ feeds.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

10. Data Protection Rights of the Individual

Data Access Requests (Subject Access Requests)

All individuals, whose data is held by us, have a legal right to request access to such data or information about what is held. We shall respond to such requests within one month and they should be made in writing to:

The Headteacher, Berry Hill Primary School, Nine Wells Road, Berry Hill, Coleford, Glos, GL16 7AT.
No charge will be applied to process the request.

Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

- Where personal data is no longer required for its original purpose, an individual can demand that the processing is stopped and all their personal data is erased by the school including any data held by contracted processors.

11. Data Security

In order to assure the protection of all data being processed and inform decisions on processing activities, we shall undertake an assessment of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them.

Risk and impact assessments shall be conducted in accordance with guidance given by the ICO:

[Risk and impact assessments | ICO](#)

Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance. The security arrangements of any organisation with which data is shared shall also be considered and where required these organisations shall provide evidence of their competence in the security of shared data.

12. Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. Berry Hill Primary School recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, Berry Hill Primary School will treat this as a data breach and will follow the personal data breach procedure.

13. Location of Information and Data

Hard copy data, records, and personal information are stored out of sight and in a locked cupboard or office. The only exception to this is medical information that may require immediate access during the school day. This will be stored with the school medical officer.

Sensitive or personal information and data should not be removed from the school site, however the school acknowledges that some staff may need to transport data between the school and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings, or are on school visits with pupils.

The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- Paper copies of data or personal information should not be taken off the school site. If these are misplaced they are easily accessed. If there is no way to avoid taking a paper copy of data off the school site, the information should not be on view in public places, or left unattended under any circumstances.
- Unwanted paper copies of data, sensitive information or pupil files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name.
- Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.
- If information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers
- Laptops and USB sticks that staff use must be password protected.

These guidelines are clearly communicated to all school staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

14. Data Disposal

The school recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.

All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process. Disposal of IT assets holding data shall be in compliance with ICO guidance:

[IT asset disposal for organisations | ICO](#)

The school uses *Print Waste* to dispose of sensitive data that is no longer required and there is a cross shredder for the purposes of shredding confidential information on-site.

15. Complaints

Complaints about how the school processes data under the GDPR and responses to subject access requests are dealt with using the School's complaints procedure.

16. Breach of Policy

Any breach of this policy should be investigated in accordance with our Data Breach process. The School will always treat any data breach as a serious issue, potentially warranting a disciplinary investigation. Each incident will be investigated and judged on its individual circumstances, addressed accordingly and carried out in line with the employee code of conduct.

17. Stop and check

As part of the ongoing training of staff, the list below has been prepared to provide a set of key 'stop and check' rules to help protect and prevent against the misuse and/or loss of data. This is not an exhaustive list but sets out some key practices that all staff should follow in their day-to-day roles at BHPS.

18. Stop and Check Rules

The most common causes of data loss or destruction are due to staff making mistakes and errors. To assist staff in the prevention of these errors occurring, below are a short set of 'stop and check' rules which will help prevent staff being the cause of data loss or destruction which can lead to significant financial and reputational harm to BHPS and its stakeholders.

BHPS asks that all staff:

STOP and CHECK before:

USING USB STICKS OR EXTERNAL STORAGE DEVICES

The use of USB Sticks or External Storage Devices is prohibited. The use of such devices poses a very real risk to the data security of BHPS and as such their use is not permitted. Transfer of files or data between devices should be undertaken using approved GCC and Microsoft Office 365 cloud storage technology such as SharePoint or OneDrive. In the very rare circumstances that the use of such a device is deemed essential, staff must use an encrypted USB stick/external storage

device. The temporary use of an encrypted device must be approved in advance of use by the Head Teacher. Staff should never use personal USB sticks or storage devices to store work related files, or send files to your personal email or other non-BHPS approved cloud services. You should never attach a non-encrypted USB stick to a computer on the BHPS network.

SAVING FILES – MAKE SURE THEY ARE ON THE APPROPRIATE COMPANY DRIVES

When saving computer files make sure that staff use the appropriate folders on the BHPS IT systems/SharePoint. Files containing personal information must not be saved on desktops or in personal folders. Files containing personal information must not be saved anywhere but SharePoint. Files that arrive via email should also be removed from emails and saved to the relevant filing system, having first ensured that the files are not malicious or contain viruses/malware (see guidance below).

RECEIVING AND OPENING EMAIL ATTACHMENTS OR DOWNLOADING FILES

BHPS has in place a number of security measures to prevent the receipt/downloading of files that may contain viruses/malware. For emails, always check the email address of the sender and type of file before opening it. If you are unsure, don't open it, speak to a member of SLT in the first instance. Phishing and viruses are very sophisticated and can even appear to have come from a trusted sender. Note the language used and type of request before responding or opening attachments to that email. If in doubt, call the person to check that the email is correct and they have genuinely sent it. For websites/download file links, always check the site is official and that you have not been inadvertently sent to a fraudulent site. Ensure the file is scanned for viruses before you open it, and never download risky file types, for example .exe files. If you have any queries regarding this, please contact a member of SLT.

SENDING EXCEL SPREADSHEETS OR OTHER DOCUMENTS WITH META DATA

Be aware of hidden content within spreadsheets (hidden rows, pivot tables, hidden data) and for other document types like Word (e.g. the properties fields).

SENDING INFORMATION

When sending personal information you should only send the minimum required amount. Create a new password protected document with the minimum information only. Don't hide Excel rows (see Rule above), as this information may still be accessible and therefore you would not be following this rule.

MAKE SURE FILES ARE PASSWORD PROTECTED

All files containing personal information must be password protected. This includes all files stored on our internal systems (SharePoint). When sending files containing personal information outside of BHPS you must ensure that these files are password protected at the file level and that the password is sent in a separate email or communication (e.g. relayed over a phone call to the recipient). Check that the method by which you are sending the files is secure and check that you have entered all details correctly before sending. Do not send files by any method which you consider not to be secure. There are certain files within school that contain personal information and confidential information regarding the school. You must ensure that these documents are password always protected and saved in the relevant file. Any file regarding pupil information must be emailed via egress.

SHARING FILES INTERNALLY

When sharing files internally which contain personal information you must do so by using the share function within Sharepoint. This ensures that you are not sending the file but a link to that file. This

link will only be accessible to employees of BHPS and provides an additional layer of protection. You must not send actual copies of files containing personal information by email.

SENDING EMAILS - ARE YOU SENDING TO THE INTENDED PERSON(S) ONLY?

Staff should make sure that you only send personal information to the intended person(s) and not to any other person by error. Email is quick and easy, but you must stop and check that you have only the correct recipients before you press send. Emails cannot be recalled or deleted.

STORING THE DATA – YOU MAY ONLY KEEP PERSONAL INFORMATION AS LONG AS PERMITTED/NECESSARY

Personal information should only be kept as long as necessary to fulfil the permitted purpose. No personal information should be kept indefinitely and should be deleted at the appropriate time in accordance with relevant statutory data retention rules.

LEAVING/STORING PHYSICAL DOCUMENTS AND DEVICES CONTAINING PERSONAL INFORMATION – GUARDING AGAINST THEFT

The first stop and check should be: Do I need to take this information out of school with me? If the answer is yes, the second stop and check should be: How will I keep this information safe? You must consider and be aware at all times where the documents/devices are and they must not be left unattended or unsecured. For example, papers should not be left on desks if those desks are unattended. If you are using documents and devices outside of school, ensure that the documents/devices containing personal information are not exposed to the public (e.g. other third parties being able to see your laptop). Theft (whether actual or inadvertent) is one of the most common causes of data loss, so remain vigilant at all times.

DESTROYING PERSONAL INFORMATION

First, check with SLT whether you should be destroying the personal information, as in certain circumstances destruction of personal information is a breach of data protection law. Secondly, make sure all documents are disposed of securely in the confidential waste bins and not thrown into a general waste bin.

LEAVING YOUR DESK - MAINTAIN A CLEAR DESK AND SHUTDOWN/LOCK YOUR DEVICES

When you are not at your desk, your desk should be clean and your device(s) screen(s) locked via password (e.g. for PC's Ctrl+Alt+Del – Lock or Windows Button + L). Personal information should never be left unsecured. You should also ensure that any work mobile or tablet is password protected and is locked whenever you are not using it.

STOP and **CHECK** before doing anything with personal information

Retention Schedule

The retention schedule below includes:

- Rationale as to why we're holding this data
- Explains if we pass this data on and, if so, once we've passed it on, if you need to keep it
- The steps we'll take when we destroy any personal data
- How long the data will be kept

CHILD PROTECTION				
RefNo	Record type	Retention action	Disposal action	Rationale / Further Info
1.1	Child protection files – CPOMS	Retain for the duration of the pupil's attendance at the school Trigger: Date pupil changes school	Transfer to new Primary school if moving in-year Transfer to Secondary School	Keeping Children Safe in Education (Department for Education) Where a child is removed from the roll to be educated at home/missing from education see below
1.2	Child protection files – CPOMS (Child missing from education, Traveller, Roma, or Gypsy and therefore removed from roll)	N/A Trigger: Date removed from roll	Transfer to Gloucestershire County Council for retention in accordance with Children's Services retention schedule	Keeping Children Safe in Education (Department for Education) Where a child is removed from the roll to be educated at home/missing from education see below
1.3	Child protection files – CPOMS (child is removed from the roll and is Elective Home Educated)	N/A Trigger: Date removed from roll	Transfer to Gloucestershire County Council for retention in accordance with Children's Services retention schedule	Keeping Children Safe in Education (Department for Education)
1.4	Allegations made against a member of staff (including unfounded allegations)	Retain until the normal retirement age for the member of staff or for 10 years (whichever is the longer) Trigger: Employee's retirement age	Do not destroy	Employment Practices Code: Supplementary Guidance (Information Commissioner's Office)
GOVERNORS				
RefNo	Record type	Retention action	Disposal action	Rationale / Further Info
2.1	Signed minutes	Retain on Gov Hub for 6 years Trigger: Date of meeting	Offer to Gloucestershire Record Office	Common practice
2.2	Agendas	No retention required Trigger: Conclusion of meeting	Destroy	Common practice
2.3	Reports	Retain on Gov Hub for 6 years Trigger: Date of report	Offer to Gloucestershire Record Office	Common practice
2.4	Instrument of Government	Retain on Gov Hub for the duration of school's operation Trigger: Closure of school	Offer to Gloucestershire Record Office	Common practice
2.5	Action Plans	Retain for 3 years Trigger: Expiration of action plan	Destroy	Common practice May be appropriate to offer to Record Office

2.6	Policy documents	Retain while policy is used operationally Trigger: Expiration of policy	Transfer to archives when policy is no longer operational	Common practice
2.7	Complaints files	Retain for 6 years Trigger: Resolution of complaint	Review and destroy if complaints are non-contentious	Common practice
2.8	Annual reports required by central government	Retain on Gov Hub at for 10 years Trigger: End of the calendar year that the record was created in	Offer to Gloucestershire Record Office	Common practice

SCHOOL LEADERSHIP & MANAGEMENT

RefNo	Record type	Retention action	Disposal action	Rationale / Further Info
3.1	Log books	Retain at school for 6 years Trigger: Date of last entry in log book	Offer to Gloucestershire Record Office	Common practice Legislation no longer requires the completion of a school log book
3.2	Minutes of senior leadership team	Retain at school for 5 years Trigger: Date of meeting	Offer to Gloucestershire Record Office	Common practice
3.3	Reports made by senior leadership team	Retain at school for 3 years Trigger: Date of report	Offer to Gloucestershire Record Office	Common practice
3.4	Improvement plans	Retain for 6 years Trigger: Expiry of plan	Review with a view to destroy	Common practice
3.5	Successful school admissions applications	Retain for 1 year Trigger: Date of admission	Destroy	Common practice
3.6	Unsuccessful school admission applications (where no appeal is made)	Retain for 1 year Trigger: Start of school term	Destroy	School Admissions Appeals Code 2022
3.7	Unsuccessful school admission applications (where an appeal is made)	Retain for 1 year Trigger: Resolution of case	Destroy	School Admissions Appeals Code 2022
3.8	Proofs of address supplied by parents as part of the admissions process	Retain for 1 year Trigger: Date of admission	Destroy	Common practice

PUPIL RECORDS

RefNo	Record type	Retention action	Disposal action	Rationale / Further Info
4.1	Admission registration form	Retain for 6 years Trigger: Last entry in register	Offer to Gloucestershire Record Office	Common practice
4.2	Attendance registers	Retain for 3 years Trigger: Last entry in register	Destroy	Common practice

4.3	Pupil files (primary school)	Retain for duration of the pupil's attendance at school Trigger: Date pupil changes school	Transfer to new Primary school if moving in-year Transfer to Secondary School	Common practice In the case of school exclusions it may be appropriate to transfer to Behaviour Service
4.4	Special educational needs records relating to individual support provided by the schools - CPOMs	Retain for duration of attendance at school Trigger: Date pupil changes school	Transfer to new Primary school if moving in-year Transfer to Secondary School	Common practice
4.5	Letters authorising or unauthorising absence - CPOMs	Retain for duration of attendance at school Trigger: Date pupil changes school	Transfer to new Primary school if moving in-year Transfer to Secondary School	Common practice
4.6	Statutory assessment test results – SIMS and INSIGHT	Retain for duration of attendance at school Trigger: Date pupil changes school	Transfer to new Primary school if moving in-year Transfer to Secondary School	Common practice
4.7	Internal school assessment results - INSIGHT	Retain for 5 years Trigger: Date of examination	Destroy	Common practice
4.8	Advice and information issued by the school to parents regarding educational needs for individual pupils - CPOMs	Retain for 12 years Trigger: Date advice issued	Transfer to new Primary school if moving in-year Transfer to Secondary School	Special Educational Needs and Disability Act 2001
4.9	Accessibility Strategy	Retain for 12 years Trigger: Expiry of strategy	Destroy	Special Educational Needs and Disability Act 2001 May be appropriate to offer to Derbyshire Record Office
4.10	Parental permission slips for school trips where there has been a major incident (e.g. involvement of emergency services, hospital admission, disease outbreak)	Retain for 25 years from the date of birth of the pupil/s involved in the incident Trigger: Pupil's date of birth	Destroy	The Limitation Act 1980
4.11	Records created by schools to obtain approval to run an Educational Visit outside the classroom where there has not been a major incident	Retain for 14 years Trigger: Date of visit	Destroy	The Health and Safety at Work Act 1974 Records created might include risk assessments

4.12	Records created by schools to obtain approval to run an Educational Visit outside the classroom where there has been a major incident (e.g. involvement of emergency services, hospital admission, disease outbreak)	Retain for 21 years from the date of birth of the pupil/s involved in the incident Trigger: Pupil's date of birth	Destroy	The Limitation Act 1980 Records created might include risk assessments
------	---	--	---------	---

CURRICULUM				
RefNo	Record type	Retention action	Disposal action	Rationale / Further Info
5.1	Curriculum development	Retain for 6 years Trigger: End of the calendar year that the record was created in	Destroy	Common practice
5.2	Curriculum Planning	Retain for 3 years Trigger: End of the calendar year that the record was created in	Review with a view to destroy	Common practice
5.3	Records of homework set	Retain for 1 year Trigger: End of the calendar year that the record was created in	Destroy	Common practice

PERSONNEL				
RefNo	Record type	Retention action	Disposal action	Rationale / Further Info
6.1	Staff personnel files	Retain for 7 years Trigger: End of employment	Do not destroy	Common practice
6.2	Recruitment record for successful candidates, including interview notes and copy evidence of entitlement to work in the UK	Retain and add to personnel file.		Common practice, Immigration, Asylum and Nationality Act 2006
6.3	Interview notes for unsuccessful candidates	Retain for 12 months Trigger: Date successful candidate is in post	Destroy	Business requirement
6.4.1	Pre-employment vetting of successful candidates, for the purposes of preventing unsuitable people from working with children (e.g. DBS checks)	Retain for 6 months Trigger: Date information checked	Destroy	DBS guidelines
6.4.2	Pre-employment vetting of successful candidates, for the purposes of ensuring school staff are adequately qualified	Add copies of evidence to personnel file (6.1)		Common practice
6.4.3	Pre-employment vetting of successful candidates, for the purposes of ensuring school staff are legally entitled to work in the United Kingdom	Add copies of evidence to personnel file (6.1)		Immigration, Asylum and Nationality Act 2006
6.5	Written warnings (level 1)	Add to personnel file (6.1)		Common practice
6.6	Written warning (level 2)	Add to personnel file (6.1)		Common practice
6.7	Final warning	Add to personnel file (6.1)		Common practice
6.8	Warnings subsequently found to be based on an unfounded case (excluding child protection related warning)	Add to personnel file (6.1)		Common practice

6.9	Staff appraisal records	Add to personnel file (6.1)		Common practice
-----	-------------------------	-----------------------------	--	-----------------

HEALTH AND SAFETY

RefNo	Record type	Retention action	Disposal action	Rationale / Further Info
7.1	Accessibility Plans, including Personal Emergency Evacuation Plan (PEEPs)	Retain for 6 years Trigger: End of the calendar year that the record was created in	Destroy	Disability and Equality Act 2010
7.2	Accident/incident reporting (adults)	Retain for 7 years Trigger: Date of incident	Destroy	Common practice
7.3	Accident/incident reporting (children)	Retain for 25 years Trigger: Child's date of birth	Destroy	The Limitation Act 1980
7.4	Records of monitoring areas where employees/pupils are likely to come into contact with asbestos	Retain for 40 years Trigger: Last action on file	Destroy	The Control of Substances Hazardous to Health Regulations 2002
7.5	Records of monitoring areas where employees/pupils are likely to come into contact with radiation	Retain for 50 years Trigger: Last action on file	Destroy	The Ionising Radiations Regulations 1985
7.6	Fire log books	Retain for 7 years Trigger: End of calendar year	Destroy	Common practice
7.7	Records of the administration of non-prescription medicines including painkillers, or very commonly prescribed drugs such as antibiotics or asthma inhalers	Retain for 1 year Trigger: End of calendar year	Destroy	Business decision Events significantly outside individual treatment plan should be treated as non-routine (see below)
7.8	Records of the administration of any other medication, including: peg feeding; injections; treatments for serious conditions such as diabetes, ADHD records of reported incidents, or problems arising from administering medication.	Retain for 21 years and 6 months from pupil's date of birth Trigger: Pupil's date of birth	Destroy	Business decision

ADMINISTRATION

RefNo	Record type	Retention action	Disposal action	Rationale / Further Info
8.1	Employer's Liability Certificate	Retain for 40 years Trigger: Closure of school		Common practice Transfer to DCC on closure of school
8.2	Inventories of equipment/furniture	Retain for 6 years Trigger: End of calendar year	Destroy	Common practice
8.3	Circulars to parents/staff/pupils	Retain for 1 year Trigger: End of calendar year	Destroy	Common practice
8.4	Newsletters produced by the school	Retain for 1 year Trigger: End of calendar year	Offer to Gloucestershire Record Office	Common practice
8.5	Paper Visitor books and sign in records	Retain for 2 years Trigger: End of calendar year	Destroy	Common practice

FINANCE

RefNo	Record type	Retention action	Disposal action	Rationale / Further Info
9.1	Annual accounts	Retain at school for 6 years Trigger: End of calendar year	Offer to Gloucestershire Record Office	Common practice
9.2	Invoices, receipts, and other financial records covered by financial regulations	Retain for 6 years Trigger: End of calendar year	Destroy	Standard financial regulations
9.3	Annual budget and supporting papers	Retain for 6 years Trigger: End of calendar year	Destroy	Common practice
9.4	Ordinary contracts	Retain for 6 years Trigger: End of contract	Destroy	The Limitation Act 1980
9.5	Contracts under seal	Retain for 12 years Trigger: End of contract	Destroy	The Limitation Act 1980

PROPERTY

RefNo	Record type	Retention action	Disposal action	Rationale / Further Info
10.1	Building plans	Retain whilst operational Trigger: End of operational use	Offer to Gloucestershire Record Office	Common practice
10.2	Burglary, theft and vandalism report forms	Retain for 6 years Trigger: End of the calendar year that the record was created in	Destroy	Common practice
10.3	Contractors' reports	Retain for 6 years Trigger: End of the calendar year that the record was created in	Destroy	Common practice

LOCAL AUTHORITY

RefNo	Record type	Retention action	Disposal action	Rationale / Further Info
11.1	Secondary transfer sheets	Retain for 2 years Trigger: Year of transfer	Destroy	Common practice
11.2	Attendance returns	Retain for 1 year Trigger: End of the calendar year that the record was created in	Destroy	Common practice
CENTRAL GOVERNMENT				
RefNo	Record type	Retention action	Disposal action	Rationale / Further Info
12.1	Ofsted reports and papers	Retain whilst current Trigger: Date new report issued	Offer to Gloucestershire Record Office	Common practice Replace old report with new report
SCH 12.2	Returns to central government (e.g. school census)	Retain for 6 years Trigger: End of the calendar year that the record was created in	Destroy	Common practice