# Data and Personal Information Protection Policy

Review Details and Document History:

| | | |
|---|---|---|
| Next review due: | May 2026 | |
| Committee responsible: | Finance | |
| Document location: | Website: | |
| | Governor hub: | Y |
| | I: Management/ Policies: | Y |

| Version | Reason for document | Date | Key changes | Current author |
|---|---|---|---|---|
| 1.0 | New doc in line with EPM model | 24.4.17 | Previously BCC policy | TJ (CD) |
| 2.0 | Updated in line with new GDPR standards | 14.5.18 | Add in responsibilities, rights to access information | TJ (CD) |
| 3.0 | Review | 13.11.20 | More information added with regard to process for data breach and Subject Access Request | AS/ TJ |
| 4.0 | GDPR audit | 4.5.21 | Amend privacy notices to One West Template | RB/TJ |
| 5.0 | Review | 11.5.23 | Data protection principles updated to latest One West | RB/TJ |
| 6.0 | Review | 23.4.25 | No changes | MO |

Contents:


1. Introduction ..... 2
2. Definitions ..... 2
3. Data Protection Principles ..... 3
4. Responsibilities ..... 5
5. Nature of Information ..... 6
6. Obtaining Information ..... 7
7. Disclosure of Information ..... 7
8. Data Breach ..... 7
9. Access to Staff Personal Files ..... 8
10. Individual rights ..... 8
11. Request for Data by Public Authorities ..... 9
12. Purposes of Information and Length of Time Retained ..... 10
13. Monitoring Activities ..... 10
14. Reporting incidents ..... 11
15. Standards of Security ..... 11
16. Training ..... 11
17. References ..... 11

Appendix A: Privacy Notices ..... 12
Appendix B: 3rd party information sharing ..... 12
Appendix C: Subject Access Request Record ..... 13
Appendix D: Data Breach Record ..... 14
Appendix E: Privacy Impact Assessment ..... 15
Appendix F: Recommended Retention of Documents ..... 16



HeadteacherMark Oldfield
Acting Deputy Headteacher: Vikki Richardson
Christ Church CE Primary School (Academy)
Royal Park, Clifton, Bristol, BS8 3AW
T: 0117 377 2830
E: christchurchp@bristol-schools.uk W:
www.christchurch.bristol.sch.uk
(Company Number 8082405)

## 1. Introduction

1.1 Christ Church School needs to keep information about our pupils, staff and other users to allow us, for example to monitor performance/achievement, Human Resources or safeguarding reasons.

1.2 The school will comply with the Data Protection Principles which are set out in the various acts relating to Data Protection.

Data Controller, Data Protection Officer and the Designated Data Protection Leads:

1.3 The school, as a body, is the Data Controller, and the Governors are therefore ultimately responsible for implementation.

1.4 The school have identified: One West as its Data Protection Officer.

1.5 The school has identified its Designated Data Leads who will deal with day to day matters as: The Head Teacher, Deputy Head Teacher, and the School Business Manager.

## 2. Definitions

2.1 Data is information which is stored electronically, on a computer, or in certain paper-based filing systems (e.g. personnel files).

2.2 Data subjects for the purpose of this policy include all living individuals about whom we hold personal data. All data subjects have legal rights in relation to their personal information.

2.3 Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name and address or date of birth) or it can be an opinion about that person, their actions and behaviour.

2.4 Data controllers are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the DPA (Data Protection Act).

2.5 Data users are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

2.6 Data processors include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions.

2.7 Processing is any activity that involves the use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring data to third parties.

2.8 **Special category** (sensitive) personal information

The School may also collect, store, and use information that falls into "special categories" of more special category personal data which has extra protection in law and requires us to identify a condition for processing under Article 9 of the GDPR.

Special category data is personal data revealing:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data for the purpose of uniquely identifying a natural person (for example fingerprints)
- data concerning health; or
- data concerning a natural person's sex life or sexual orientation

The Article 9 grounds which we may rely on to process special category data include:

- Legal obligation
- Substantial public interest including:
    - Statutory and government purposes
    - Equality of opportunity or treatment
    - Preventing and detecting unlawful acts
    - Preventing fraud
    - Public Health
    - Safeguarding
- Support for individuals with a particular disability or medical condition
- Explicit consent, for example to the use of biometric data, e.g. fingerprints.
- To maintain your vital interests

## 3. Data Protection Principles

GDPR is based on 7 key data protection principles that the school complies with.

The principles say that personal data must be:

3.1 **Processed lawfully, fairly and in a transparent manner** – the school will explain to individuals why the school needs their data and why it is processing it – for example on consent forms (where consent is used as the basis for processing), and in its Privacy Notice(s). The school reviews its documentation and the basis for processing data on a regular basis

3.2 **Collected for specified, explicit and legitimate purposes** – the school explains these reasons to the individuals concerned when it first collects their data. If the School wishes to use personal data for reasons other than those given when the data was first obtained, it will inform the individuals concerned before doing so, and will seek consent where necessary and appropriate unless the new purpose is compatible with that in respect of which consent was given, or there is another lawful basis for sharing the information. The School will document the basis for processing.

3.3 **Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed** - the school must only process the minimum amount of personal data that is necessary in order to undertake its work.

3.4 **Accurate and, where necessary, kept up to date** – the School will check the details of those on its databases at appropriate intervals and maintain the databases. It will consider and respond to requests for inaccurate data to be rectified in accordance with the Data Protection Act 2018.

3.5 **Kept for no longer than is necessary for the purposes for which it is processed** – We review what data we hold at appropriate intervals – for example upon the annual review of the Record of Processing Activities (or sooner if needed). When the School no longer needs the personal data it holds, it will ensure that it is securely deleted or anonymised in accordance with the retention schedule. We only keep personal data, include special category data in an identifiable form for as long as is necessary for the purposes for which it was collected, or where there is a legal obligation to do so.

3.6 **Processed in a way that ensures it is appropriately secure** – the School implements appropriate technical measures to ensure the security of data and systems for staff and all users.

A risk- based approach is taken to taking data offsite. Electronic personal data with lower sensitivity may be taken off site stored on a school laptop or on the school secure drive. All devices used to access data must be secured with the school's IT multi factor authentication. Unless absolutely necessary, hard copies of special category personal data will not be removed from our premises. If there is no reasonable alternative to removing hard copies from the school site, the following procedure will apply:

- Hard copy personal data with lower sensitivity (e.g. exercise books) may be taken off site, but if left in a vehicle must be locked in the boot, never left in a visible place, only for the shortest period of time and never overnight. Data will be tidied away when not in use (e.g. when staff undertake marking at home, it must be out of sight of family members, not left out and tidied away afterwards).
- Hard copy data (e.g. lists of names to be taken off site on for example a school trip) will be kept on a staff member's person throughout the day and shredded at the end of the school day.
- Special Category Data (e.g. SEND, Safeguarding, Health data) must be kept on the staff member's person at all times.
- Special category data must be returned to the School's premises at the end of the working day
- Only those who have need to access the data concerned will be granted permission and access to it.

3.7 **Accountability** – The School complies with its obligations under data protection laws including the GDPR and can demonstrate this via the measures set out in this policy including:

- Completing Data Protection Impact Assessments (DPIAs) where the School's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies. This largely involves special category personal data. However, the School will liaise with the DPO who will advise on this process. Any activity involving the processing of personal data must be registered on the Register of Processing Activity and reviewed, at the very least, annually
- Integrating data protection into internal documents including this policy, any related policies and Privacy Notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters. Staff who process special category data will be provided with such additional training as appropriate for example on safeguarding systems. Records of training are maintained
- Regularly conducting reviews and audits to test its privacy measures and ensure compliance with relevant legislation and school policies
- Maintaining records of its processing activities for all personal data that it holds
- Policies related to the handling of data and associated documentation will be regularly reviewed on a rolling basis and updated in accordance with new guidance, legislation and practice. They will be publicised to staff who will be required to familiarise themselves with them
- The Record of Processing Activities will be maintained and reviewed at least annually
- Where any breaches of personal data have occurred, the reasons for this will be reviewed and changes made to practice and procedure as appropriate
- Stakeholders will manage risks and compliance using the annual compliance statement provided by the Data Protection Officer

## 4. Responsibilities

4.1 Responsibilities of the School:

The school is committed to protecting and respecting the confidentiality of sensitive information relating to staff, pupils, parents and governors. This implies that:

a) all systems that involve personal data or confidential information will be examined to see that they meet the Data Protection Principles and Information Security guidelines

b) the school will inform all users about their rights regarding data protection

c) the school will provide training to ensure that staff know their responsibilities

d) the school will monitor its Data Protection and Information Security processes on a regular basis, changing practices if necessary.

e) systems and staff data processing will be audited once a year internally (by a Data Protection Lead and the Data Protection Governor) and once a year externally (by the Data Protection Officer)

f) a statement of intent (Privacy Notice) with regard to collection, processing, retrieval and deletion of data for both pupils and staff is listed in Appendix A and is published on the school website

4.2 Responsibilities of Staff:

All staff are responsible for checking that any information that they provide to the school about their employment is accurate and up to date.

All staff are also responsible for ensuring that any personal data they use in the process of completing their role:

a) is not in the view of others when being used

b) is kept securely in a locked filing cabinet or drawer when not being used

c) be password protected both on a local hard drive and on a network drive that is regularly backed up

d) USB sticks or other removable storage media are considered un-secure and are not used for processing school data

e) is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

f) Any photo or recording taken on school or personal devices should be downloaded immediately to the school secure drive and deleted from the device before leaving the school site.

Staff should note that unauthorised disclosure or transgression of the above statements will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Staff will be required to read and sign an annual Code of Conduct which will include the principles of data protection.

4.3 Responsibilities of Parents/Guardians:

The school will inform the Parents/Guardians of the importance and how to make any changes to personal data. This includes an annual data collection sheet within the Home School Agreement which will be issued yearly and the collection recorded.

Other permissions will also be sought regarding matters such as the use of images and use of names in publicity materials on induction, annually or when required. The returns to these permissions will be verified and exemptions communicated to staff.

4.4 Responsibilities of Governors:

All Governors will be required to uphold the principles of data protection and to sign an annual Code of Conduct for Governors.

A Governor will be appointed annually as the Data Protection Governor and will be responsible for ensuring the principles of data protection are being upheld by the school. They will review once a year the data protection systems and documentation; support the annual audit of the systems and support the school on any subject access requests or data breaches.

## 5. Nature of Information

5.1 We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

5.2 We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

## 6. Obtaining Information

6.1 We will process data about staff for legal, personnel, administrative and management purposes and to enable us to meet our legal obligations as an employer, for example to pay, monitor performance and to confer benefits in connection with employment.

6.2 We may process special category personal data relating to staff including, as appropriate:

a) information about an employee's physical or mental health or condition in order to monitor sick leave and take decisions as to the employee's fitness for work;
b) the employee's racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;
c) in order to comply with legal requirements and obligations to third parties.

## 7. Disclosure of Information

7.1 Personal data will be used only for the purpose for which it was gathered, unless the consent of the people concerned has been obtained to a new or varied use.

7.2 Where the school collects data regularly, it will state what the data is and ask for consent to use it in the manner deemed necessary.

7.3 In other cases, the explicit consent of the data subject will be obtained in writing. Confirmation of consent by telephone is acceptable if a written request has been received which implies the consent of the data subject.

7.4 Access to personal data will be refused if the data user is uncertain whether the person requesting access, including another member of staff, is entitled to it.

7.5 Data will be routinely shared with the following 3rd parties as part of our contracted educational service – see below. Data is stored on approved education databases as listed in Appendix C or sent through encrypted communications.

- schools that the pupil's attend after leaving us
- our local authority
- the Department for Education (DfE)

## 8. Data Breach

8.1 If we discover that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, the Data Protection Officer will report it to the Information Commissioner within 72 hours of discovery.

8.2 If the breach is likely to result in a high risk to the rights and freedoms of individuals, all affected individuals will be informed of the breach and provided with information including the type of data and likely consequences of the breach, plus mitigating steps taken.

8.3 Any breach of the policy will be fully investigated and remedial steps taken to ensure a similar breach cannot happen again.

8.4 A record of all data breaches, regardless of their size or effect, will be retained within the Breach Register, as set out in Appendix E of this Policy & available from the Data Protection Officer.

## 9. Access to Staff Personal Files

9.1 Staff are entitled to know if the school holds information about them and must make a formal written request for information held about them addressed to the Headteacher or Chair of Governors.

9.2 Information which would disclose the identity of a third person is exempt from access, unless the consent of the source is available or it is reasonable in all the circumstances to comply with the subject access request without the third party's consent under section 7 of the DPA. Personal data may be exempt for other reasons under the DPA.

9.3 Requests for access to personal data will be dealt with within 1month (or 3 months if complex) of receipt of sufficient information to process the request.

## 10. Individual rights

As a data subject, individuals have a number of rights in relation to personal data.

10.1 Subject access requests

Individuals have the right to make a subject access request (SAR). If an individual makes a subject access request, the school will fill in a SAR form (App D) to tell them:

- whether or not their data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom their data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to transfers;
- for how long their personal data is stored (or how that period is decided);
- their rights to rectification or erasure of data, or to restrict or object to processing;
- their right to complain to the Information Commissioner if they think the organisation has failed to comply with their data protection rights; and
- whether or not the organisation carries out automated decision-making and the logic involved in any such decision-making.

10.2 The school will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless they agree otherwise.

10.3 If the individual requests additional copies, the school reserves the right to charge a fee, which will be based on the administrative cost to the organisation of providing the additional copies.

10.4 To make a subject access request, the individual should send the request to the school email address christ.church.p@bristol-schools.uk (if a SAR request is made verbally, the school should ask the individual to follow this up with a written request to the school email address). The school may need to verify the identification of the individual before the request can be processed. The school will inform the individual if it needs to verify their identity and the documents it requires.

10.5 The school will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the school processes large amounts of the individual's data, it may respond within three months of the date the request is received. The school will write to the individual within one month of receiving the original request to tell them if this is the case.

10.6 If a subject access request is manifestly unfounded or excessive, the school is not obliged to comply with it. Alternatively, the school can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the school has already responded. If an individual submits a request that is unfounded or excessive, the school will notify them that this is the case and whether or not it will respond to it.

10.7 Other rights

Individuals have a number of other rights in relation to their personal data. They can require the school to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the school's legitimate grounds for processing data (where the school relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the school's legitimate grounds for processing data.

To ask the school to take any of these steps, the individual should send the request to the school email address christ.church.p@bristol-schools.uk.

10.8 There is a separate policy for the processing of Freedom of Information requests.

## 11. Request for Data by Public Authorities

11.1 Requests for personal data may come from public authorities, including but not limited to the following:

- the Police;
- the Department of Work and Pensions;

- the UK Border Agency;
- HM Revenue & Customs;
- Local Authorities;
- DVLA.

11.2 Requests received from a public authority will only be processed when submitted in writing, including electronic communication. Such requests for data usually require that the organisation does not inform, or gather consent from, the data subject when responding to the request. When a request is received, this should first be referred to the Data Protection Officer who will ensure that the request is valid.

11.3 Data can only be disclosed without the knowledge and consent of the data subject where it is processed for either the:

- prevention or detection of crime;
- apprehension or prosecution of offenders; or
- assessment or collection of tax or duty.

11.4 Additionally, it must be shown that informing or gathering consent from the data subject would likely prejudice the crime or taxation purposes.

11.5 Where these conditions are not met, the Data Protection Officer may decide to not disclose the data. Where the Data Protection Officer decides the records should not be disclosed or only partially disclosed, they must record in writing their reasons. A public authority may have a Court Order issued for the disclosure of documents. Any objections should be recorded along with the Court Order however the data should be disclosed.

## 12. Purposes of Information and Length of Time Retained

Data will be held as indicated in Appendix G. We will not keep personal data longer than necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy or erase from our systems, all data which is no longer required.

## 13. Monitoring Activities

13.1 The school will record and monitor usage of all company IT equipment, user activity, voice traffic, email and internet usage as deemed necessary.

13.2 Those responsible for undertaking the monitoring will observe the strictest confidentiality when undertaking these activities. The report will be made directly to the School Business Manager, who will determine any action that may need to be taken.

13.3 Monitoring of IT equipment, electronic data, telephone calls, emails, internet access, network access and remote access will be carried out to ensure that usage is in accordance with One West policies, procedures and guidelines.

## 14. Reporting incidents

Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal data about himself or herself or their child should raise the matter with the Head Teacher, in the first instance.

## 15. Standards of Security

The School will determine and maintain an appropriate level of security (and back–up) for its premises, equipment, network, programs, data and documentation, and will ensure that access to them is restricted to appropriate staff. Sensitive data will be stored in secure locations – lockable cupboards or restricted electronic storage.

Any data breaches will be recorded in a Data Breach Record (see Appendix E), the DPO (Data Protection Officer) notified, and the ICO (information commissioner's office) notified if deemed necessary by the DPO.

Any new project undertaken by the school that involves data, will be analysed through a Privacy Impact Assessment (see Appendix F) before progressing.

## 16. Training

All employees who handle personal data will receive training on data protection procedures, which includes information about the standards the School expects its employees to observe in the use of personal data. Induction of new staff will include necessary reference to data protection.

## 17. References

The Governing Body will comply with DfE guidance on references as amended from time to time in particular in relation to safeguarding children and safer recruitment in education.

## Appendix A: Privacy Notices

**How we use pupil and parent/carer information** - Please see Privacy Notice – Pupils and Parents/ Carers – located on website at: https://christchurchps.schoolzineplus.co.uk/policies

**How we use school workforce information** - Please see Privacy Notice – School Workforce – located on website at: https://christchurchps.schoolzineplus.co.uk/policies

**How we use job applicant information** - Please see Privacy Notice – Job Applicants – located on website at: https://christchurchps.schoolzineplus.co.uk/policies

## Appendix B: 3rd party information sharing

*Organisations with which we share pupil, staff or governor information either for the purposes of data storage or national education operation:*

Department of Education
Bristol Local Authority
Schools which pupils have come from or are going to
School catering
School wrap around care
Companies House
HR & Payroll Provider
Accountancy provider
External education professionals
School photographer
External trips and residential camps
Legal provider
IT provider
Website provider
Financial packages
Governor portal
Pupil database
Pupil assessment database
Payment portal

## Appendix C: Subject Access Request Record

Name of data subject: _____

Name of person who made request: _____

Date request received: ____/____/____

Contact DPO: ____/____/____

Date acknowledgement sent: ____/____ /____

Name of person dealing with request: _____

| | Notes (Overwrite the statements in grey) |
|---|---|
| Are they entitled to the data? Does their identity need to be verified? | If no reply stating reasons and/or ask for proof |
| Do you understand what data they are asking for? Clarify. Timescales do not start until identity and content have been clarified. | If no, ask requestor for clarity |
| Identify the data | What data sources, where they are kept |
| Collect the data required (is the data simple – 1month preparation period, or complex – 3month preparation period) | You may need to ask others – state a deadline in your request. |
| Do you own all the data? | If no, ask third parties to release external data. If data is supplied by another agency such as Psychology Service, you do not own the data. |
| Do you need to exempt/redact data? | If exempting/redacting be clear of your reasons<br>Document name, data exempted/redacted, why. |
| Is the data going to be ready in time? | Record delays and reasons.<br>Communicate with requestor stating reason for delay and asking if they would like the data you have collected so far. |
| Create pack | Make sure that the data is in an easy to access format: paper, word, excel etc. |
| Inform requestor you have the data | Ask them how they would like it delivered |
| Deliver data | Ask for confirmation/special delivery? |

At all stages your DPO or Data Protection lead will be able to provide you with advice.

Date request completed: ____/____/____

(within 1month or 3months depending on complexity of request)

Signed off by: _____

## Appendix D: Data Breach Record

| | | | | | |
|---|---|---|---|---|---|
| Date: / / | Person responsible for dealing with breach | | | | |
| Outline of breach | | | | | |
| Which data subjects are involved | | | | | |
| Data type involved | | | | | |
| Reported by | | | | | |
| Phone/email sent to DPO | y/n | Is this high risk? | y/n | Report to ICO | y/n |
| Date reported to data subjects | | | | | |
| Actions taken | | | | | |
| Preventative action suggestions – including training | | | | | |
| Notes | | | | | |
| Actions approved by | | Date | / / | | |

## Appendix E: Privacy Impact Assessment

| |
|---|
| What is the aim of the project? |
| |
| What data will be collected? |
| |
| How will the data be collected? |
| |
| Where will the data be stored? |
| |
| How will the data be shared? |
| |
| How will the data be amended or deleted? |
| |
| Identified risks (Issues, Risk to individuals, Compliance Risk, School Risk, Possible Solution) |
| |
| Signed Off by: Date: |

HeadteacherMark Oldfield
Acting Deputy Headteacher: Vikki Richardson
Christ Church CE Primary School (Academy)
Royal Park, Clifton, Bristol, BS8 3AW
T: 0117 377 2830
E: christchurchp@bristol-schools.uk W:
www.christchurch.bristol.sch.uk
(Company Number 8082405)



Member of the NW24 Teaching & Learning Partnership

## Appendix F: Recommended Retention of Documents

| File description | Retention Period | Stored | Action at end of retention period |
|---|---|---|---|
| **Child Protection** | | | |
| Child Protection files | DOB + 25 years | Headteacher office, School office cupboard files, management drive | SHRED/ DELETE by Office<br>Child Protection information must be copied and sent under separate cover to new school/college whilst the child is still under 18 (i.e. the information does not need to be sent to a university for example)<br>Where a child is removed from roll to be educated at home, the file should be copied to the LA. |
| Allegation of a child protection nature against a member of staff, including where the allegation is unfounded | Until the person's normal retirement age, or 10 years from the date of the allegation if that's longer | Headteacher office | SHRED/ DELETE by Office<br>Employment Practices Code: Supplementary Guidance :<br>"Records of allegations about workers who have been investigated and found to be without substance should not normally be retained once an investigation has been completed. There are some exceptions to this where for its own protection the employer has to keep a limited record that an allegation was received and investigated, for example, where the allegation relates to abuse and the worker is employed to work with children or other vulnerable individuals" |
| **Governors** | | | |
| Minutes | Retain in school for 6 years from date of meeting | Governor Hub/ Management drive/ website (for main FGB minutes) | SHRED/ DELETE by Clerk / SBM |
| Agendas | Date of meeting + 1 year | Governor Hub/ Management drive | SHRED/ DELETE by Clerk / SBM |
| Reports | Date of report + 6 years | Governor Hub/ Management drive | SHRED/ DELETE by Clerk / SBM |
| Instruments of Government | Permanent | Management drive/ SBM cupboard | Retain in school whilst school is open |
| Trusts and Endowments | Permanent | Management drive/ SBM | Retain in school whilst operationally required |

| File description | Retention Period | Stored | Action at end of retention period |
|---|---|---|---|
| | | cupboard | |
| Action Plans | Date of action plan + 3 years | Governor Hub/ Management drive | SHRED/ DELETE by Clerk / SBM |
| Policy documents | Expiry of policy | Governor Hub/ Management drive/ staffroom policies folder/ SBM cupboard | SHRED/ DELETE by Clerk / SBM |
| Complaints files | Date of resolution of complaint + 6 years | Governor Hub/ Governor email | SHRED/ DELETE by Clerk |
| Annual Reports required by the Department for Education and Skills | Date of report + 10 years | Governor Hub/ Management drive | SHRED/ DELETE by Clerk / SBM |
| **Management** | | | |
| Log Books (Books where the Head-teacher or another member of staff keeps of record of what happens in the school, this may include details of events, photographs and other information) | Date of last entry in the book + 6 years | SLT Offices | SHRED/ DELETE by relevant member of SLT |
| Minutes of the Senior Management Team and other internal administrative bodies | Date of meeting + 5 years | SLT Offices / Management Drive | SHRED/ DELETE by SBM/ Headteacher |
| Reports made by the head teacher or the management team | Date of report + 3 years | SLT Offices / Management Drive | SHRED/ DELETE by SBM/ Headteacher |
| Records created by head teachers, deputy head teachers, and other members of staff with administrative responsibilities (except child protection records which are dealt with above). | Closure of file + 6 years | SLT Offices / Management Drive | SHRED/ DELETE by SBM/ Headteacher |
| Correspondence created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities | Date of correspondence + 3 years | SLT Offices / Management Drive | SHRED/ DELETE by SBM/ Headteacher |
| Professional development plans | Closure + 6 years | SLT Offices / Management Drive | SHRED/ DELETE by SBM/ Headteacher |
| School development plans | Closure + 6 years | Governor Hub / Management Drive | SHRED/ DELETE by SBM/ Headteacher |
| **Pupils** | | | |
| Admission Registers | Date of last entry in the book (or file) + 6 years | Office cupboard/ Managemer drive | SHRED/ DELETE by School Office |

| File description | Retention Period | Stored | Action at end of retention period |
|---|---|---|---|
| Attendance registers | Date of register + 3 years | Office cupboard/ Management drive/ SIMS | SHRED/ DELETE by School Office |
| Pupil record cards | Retain for the time which the pupil remains at the primary school | Office cupboard/ Management drive/ SIMS | Transfer to the secondary school (or other primary school) when the child leaves the school. In the case of exclusion it may be appropriate to transfer the record to the Behaviour Service |
| Pupil files | Retain for the time which the pupil remains at the primary school | Office cupboard/ Management drive | Transfer to the secondary school (or other primary school) when the child leaves the school. In the case of exclusion it may be appropriate to transfer the record to the Behaviour Service |
| Special Educational Needs files, reviews and Individual Education Plans | DOB of the pupil + 25 year | SEN cupboard/ Management drive | SHRED/ DELETE by School Office |
| Letters authorising absence | Date of absence + 2 years | SIMS | SHRED/ DELETE by School Office |
| Absence books | Current year + 6 years | Office cupboard | SHRED/ DELETE by School Office |
| Examination results: | | | |
| *Public* | Year of examinations + 6 years | Teacher's drive, Teacher cupboards | SHRED/ DELETE by School Office |
| *Internal* | Current year + 5 years | SPTO, Teacher's drive, Teacher cupboards | SHRED/ DELETE by School Office |
| Any other records created in the course of contact with pupils | Current year + 3 years | Teacher's drive, Teacher cupboards, Office cupboard pupil files, management drive | Review at the end of 3 years and decide whether to retain for a further period or SHRED/ DELETE by School Office |
| Statement maintained under The Education Act 1996 - Section 324 | DOB + 30 years | SEN cupboard/ Management drive | SHRED/ DELETE by School Office unless legal action is pending |
| Proposed statement or amended statement | DOB + 30 years | SEN cupboard/ Management drive | SHRED/ DELETE by School Office unless legal action is pending |
| Advice and information to parents regarding educational needs | Closure + 12 years | SEN cupboard/ Management drive | SHRED/ DELETE by School Office unless legal action is pending |
| Accessibility Strategy | Closure + 12 years | SEN cupboard/ Management drive | SHRED/ DELETE by School Office unless legal action is pending |
| Children SEN Files | Closure + 35 years | SEN cupboard/ Management drive | SHRED/ DELETE by School Office unless legal action is pending |

| File description | Retention Period | Stored | Action at end of retention period |
|---|---|---|---|
| **Curriculum** | | | |
| Curriculum development | Current year + 6 years | Teacher's drive/ Teacher books/ cupboards/ Website | SHRED/ DELETE by Teachers |
| Curriculum returns | Current year + 3 years | Teacher's drive/ Teacher books/ cupboards/ | SHRED/ DELETE by Teachers |
| School syllabus | Current year + 1 year | Teacher's drive/ Teacher books/ cupboards/ Website | SHRED/ DELETE by Teachers |
| Schemes of work | Current year + 1 year | Teacher's drive/ Teacher books/ cupboards/ | SHRED/ DELETE by Teachers |
| Timetable | Current year + 1 year | Teacher's drive/ Teacher books/ cupboards/ | SHRED/ DELETE by Teachers |
| Class record books | Current year + 1 year | Teacher's drive/ Teacher books/ cupboards/ | Review at the end the retention period and decide whether to retain for a further period or SHRED/ DELETE by School Office |
| Mark Books | Current year + 1 year | Teacher books/ cupboards/ | Review at the end the retention period and decide whether to retain for a further period or SHRED/ DELETE by School Office |
| Record of homework set | Current year + 1 year | Teacher's drive/ Teacher books/ cupboards/ | SHRED/ DELETE by Teachers |
| Pupils' work | Current year + 1 year | Pupil drive/ Teacher books/ cupboards/ displays | Review at the end the retention period and decide whether to retain for a further period or SHRED/ DELETE by School Office |
| **Personnel** | | | |
| Timesheets, sick pay | Current year + 6 years | SBM cupboard/ EPM portal/ Management Drive | SHRED/ DELETE by SBM |
| Staff Personnel files | Termination + 7 years | SBM cupboard/ EPM portal/ Management Drive | SHRED/ DELETE by SBM |
| Interview notes and recruitment records | Date of interview + 6 months | SBM cupboard/ Management Drive | SHRED/ DELETE by SBM |
| Pre-employment vetting information (including unsuccessful CRB checks) | Date of check + 6 months | SBM cupboard/ Management Drive | SHRED/ DELETE by SBM for unsuccessful candidates, place on personnel file for successful candidate |
| Disciplinary proceedings for all matters **except** those relating to child protection issues (see above): | | | |
| *oral warning* | Date of warning + 6 months | SBM cupboard/ Management Drive | SHRED/ DELETE by SBM – if placed on personnel file, should be weeded from file |

| File description | Retention Period | Stored | Action at end of retention period |
|---|---|---|---|
| *written warning – level one* | Date of warning + 6 months | SBM cupboard/ Management Drive | SHRED/ DELETE by SBM – if placed on personnel file, should be weeded from file |
| *written warning – level two* | Date of warning + 12 months | SBM cupboard/ Management Drive | SHRED/ DELETE by SBM – if placed on personnel file, should be weeded from file |
| *final warning* | Date of warning + 18 months | SBM cupboard/ Management Drive | SHRED/ DELETE by SBM – if placed on personnel file, should be weeded from file |
| *case not found* (except child protection allegatio see above) | DESTROY immediately at the conclusion of the case | SBM cupboard/ Management Drive | SHRED/ DELETE by SBM |
| Records relating to accident/injury at work | Date of incident + 12 years | Office cupboard (premises book), Management Drive. SBM cupboard | Review at the end the retention period and decide whether to retain for a further period or SHRED/ DELETE by SBM |
| Annual appraisal/assessment records | Current year + 5 years | Headteacher cupboard, Management Drive | SHRED/ DELETE by SBM/ Headteacher |
| Salary cards | Last date of employment + 6 years | SBM cupboard/ Management Drive, EPM portal | SHRED/ DELETE by SBM |
| Maternity pay records | Current year, +3yrs | SBM cupboard/ Management Drive, EPM portal | SHRED/ DELETE by SBM |
| Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995 | Last payment + 6 years | SBM cupboard/ Management Drive, EPM portal | SHRED/ DELETE by SBM |
| **Health and Safety** | | | |
| Accessibility Plans | Current year + 6 years | Office cupboard (premises book), management drive | SHRED/ DELETE by SBM |
| Accident Reporting | | | |
| *Adults – Accident Book* | Last entry in the accident book + 3 years | Office cupboard (premises book), management drive, accident book | SHRED/ DELETE by SBM |
| *Adults – Internal Reports* | Current year + 3 years | Office cupboard (premises book), management drive, accident book | SHRED/ DELETE by SBM |
| *Children* | DOB + 25 years | Office cupboard (premises book), management drive, accident book, pupil files | SHRED/ DELETE by SBM |

| File description | Retention Period | Stored | Action at end of retention period |
|---|---|---|---|
| | | (office cupboard, SIMS) | |
| COSHH | Current year + 10 years | Office cupboard (premises book), management drive | SHRED/ DELETE by SBM |
| Incident reports | Current year + 20 years | Office cupboard (premises book), management drive | SHRED/ DELETE by SBM |
| Policy Statements | Date of expiry + 1 year | Office cupboard (premises book), management drive | SHRED/ DELETE by SBM |
| Risk Assessments | Date assessment superseded + 3 years | SBM cupboard/ Management Drive | SHRED/ DELETE by SBM |
| Process of monitoring of areas where employees and persons are likely to have come in contact with **asbestos** | Last action + 40 years | SBM cupboard/ Management Drive | SHRED/ DELETE by SBM |
| Fire Precautions log books | Current year + 6 years | Office cupboard (premises book), management drive | SHRED/ DELETE by SBM |
| **Administrative** | | | |
| Employer's Liability certificate | Permanent whilst the school is open, changes annually | SBM noticeboard, management drive | Retain for 40 years after school has closed |
| Inventories of equipment and furniture | Disposal of last item + 6 years or date superseded + 6 years | Management drive | SHRED/ DELETE by SBM |
| General file series | Current year + 5 years | Management drive | SHRED/ DELETE by SBM |
| School brochure/prospectus | Current year + 3 years | Management drive | SHRED/ DELETE by SBM |
| Circulars (staff/parents/pupils) | Current year + 1 year | Management drive/ Governor hub | SHRED/ DELETE by SBM |
| Newsletters | Current year + 1 year | Management drive/ staffroom folder/ SBM cupboard/ website | Review at the end the retention period and decide whether to retain for a further period or SHRED/ DELETE by SBM |
| Visitors' book | Current year + 2 years | Office cupboard/ Management drive | Review at the end the retention period and decide whether to retain for a further period or SHRED/ DELETE by SBM |
| PTA/Old Pupils' Associations | Current year + 6 years | Email | Review at the end the retention period and decide whether to retain for a further period or SHRED/ |

| File description | Retention Period | Stored | Action at end of retention period |
|---|---|---|---|
| | | | DELETE by SBM |
| **Finance** | | | |
| Annual Accounts | Current year + 6 years | SBM cupboard, Management drive, Governor Hub, website | SHRED/ DELETE by SBM |
| Loans and grants | Date of last payment on loan + 12 years | Management drive | Review at the end the retention period and decide whether to retain for a further period or SHRED/ DELETE by SBM |
| Contracts | Contract completion date + 6 years | Management drive, SBM cupboard | SHRED/ DELETE by SBM |
| Budget reports, budget monitoring etc | Current year + 2 years | Management drive, budgeting portal, Governor hub | SHRED/ DELETE by SBM |
| Invoice, receipts and other records covered by the Financial Regulations | Current year + 2 years | Financial package, Office cupboard, Management drive | SHRED/ DELETE by SBM |
| Annual Budget and background papers | Current year + 3 years | Management drive, Governor hub | SHRED/ DELETE by SBM |
| Order books and requisitions | Current year + 6 years | Financial package, Office cupboard, Management drive | SHRED/ DELETE by SBM |
| Delivery Documentation | Current year + 6 years | Office cupboard, Management drive | SHRED/ DELETE by SBM |
| Debtors' Records | Current year + 6 years | Financial package, Office cupboard, Management drive | SHRED/ DELETE by SBM |
| Applications for free school meals, travel, uniforms etc | Current year + 6 years | Office cupboard, Management drive | SHRED/ DELETE by SBM |
| Free school meals registers | Current year + 6 years | Office cupboard, Management drive | SHRED/ DELETE by SBM |
| Petty cash books | Current year + 6 years | Office cupboard, Management drive | SHRED/ DELETE by SBM |
| **Property** | | | |
| Title Deeds | Permanent | Management drive, SBM cupboard | These should follow the property |

| File description | Retention Period | Stored | Action at end of retention period |
|---|---|---|---|
| Plans | Permanent | Management drive, SBM cupboard | Retain until superseded and then SHRED/ DELETE by SBM |
| Maintenance and contractors | Current year + 6 years | Management drive, SBM cupboard | SHRED/ DELETE by SBM |
| Leases | Expiry of lease + 6 years | Management drive | SHRED/ DELETE by SBM |
| Lettings | Current year + 3 years | Management drive | SHRED/ DELETE by SBM |
| Burglary, theft and vandalism report forms | Current year + 6 years | Management drive | SHRED/ DELETE by SBM |
| Maintenance log books | Last entry + 10 years | School office cupboard (premises book), management drive | SHRED/ DELETE by SBM |
| Contractors' Reports | Current year + 6 years | Management drive | SHRED/ DELETE by SBM |
| **DfE** | | | |
| OFSTED reports and papers | Replace former report with any new inspection report | Management drive, Governor hub, website | Review at the end the retention period and decide whether to retain for a further period or SHRED/ DELETE by SBM |
| Returns | Current year + 6 years | Management drive | SHRED/ DELETE by SBM |
| **School Meals** | | | |
| Dinner Register | Current year + 3 years | School office cupboard, management drive | SHRED/ DELETE by School Office |
| School Meals Summary Sheets | Current year + 3 years | School office cupboard, management drive | SHRED/ DELETE by School Office |