Inter-School
Data Protection Policy (GDPR)

School of Christ the King Hartcliffe Rd Bristol BS4 1HD	St Bernadette RC Primary Gladstone Road Bristol BS14 9LP	Holy Cross RC Primary School Dean Lane Bristol BS3 1DB

Please note, any reference to "School" refers to all of the schools above.
This policy has been ratified by the Governing body of all 3 schools on the date noted below.

Review Date: March 2026

Next Review Date: March 2027

Statutory policy - Annual Review

Source of policy: St Bernadette Secondary

History: 2018

Amendments:

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, carers, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill. This is in keeping with our School Mission Statement.
This policy applies to all personal data, regardless of whether it is in paper, electronic or any other format.

- **2. Legislation and guidance**

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

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 code of practice 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.

- **3. Definitions**

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: ● Name (including initials) ● Identification number ● Location data ● Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: Racial or ethnic origin Political opinions Religious or philosophical beliefs Trade union membership Genetics

	Health – physical or mental Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

- **4. The data controller**

"The School" processes personal data relating to parents, carers, pupils, staff, governors, visitors and others, and therefore is a data controller.
The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

- **5. Roles and responsibilities**

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy will face disciplinary action.

5.1 Governing body

The governing body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing body and, where relevant, report to them their advice and recommendations on school data protection issues.
The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.
Full details of the DPO's responsibilities are set out in their job description.
Our DPO is Mr J Franks and is contactable via the email address dpo@holycross.bristol.sch.uk

5.3 Headteacher

The Headteacher acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
- With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
- If they have any concerns that this policy is not being followed
- If they are unsure whether or not they have a lawful basis to use personal data in a particular way
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The GDPR is based on data protection principles that our school must comply with.
The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- 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**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent when the pupil is under 13 (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

The school will inform parents/carers of all pupil data they collect, process and hold on pupils, the purposes for which the data is held and the third parties to whom it may be passed. This information is available in a privacy notice which will be available to pupils and parents / carers through the school website with a hard copy available from the school office.

The Privacy Notices for "The School" can be found as Appendix 1 in this policy.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's Data Retention Schedule (Appendix 2).

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, our external catering company. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations

- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

  We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

  Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

  Subject access requests must be submitted in writing by completion of the Subject Access Request Form (Appendix 3) to the DPO.

  If staff receive a subject access request they must immediately forward it to the DPO.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

  We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 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 (see section 7), 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 (See Appendix 4 – Right to be Forgotten Form)
- 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)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

- **10. Parental requests to see the educational record**

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

- **12. CCTV**

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to Mr J Franks – Data Protection Officer.

- **13. Photographs and videos**

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

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, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will remove the photograph or video and not distribute it further, or we will remove the name and blur out the child's face.

See our ICT Acceptable Use Policy - Staff for more information on our use of photographs and videos.

- **15. Data protection by design and default**

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- 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; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
- For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
- For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

- **16. Data security and storage of records**

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept secure when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access

- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff are reminded to change their passwords at regular intervals
- Portable devices such as USB data Sticks or removable media are only to be used for planning where no data is involved.
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our ICT Acceptable Use Policy - Staff on acceptable use)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

- **17. Disposal of records**

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

18. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 6.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

- **19. Training**

All staff and governors are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

- **20. Monitoring arrangements**

The DPO is responsible for monitoring and reviewing this policy. It will be approved by the Resources Committee of the Governing Body.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill

that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **every year** by the Finance and Premises Committee and shared with the Full Governing Body.

- **21. Links with other policies**

This data protection policy is linked to our:

- Freedom of Information Publication Scheme
- Online Safety Policy
- Safeguarding and Child Protection Policy
- ICT Acceptable Use Policies
- Staff Code of Conduct
- Staff Disciplinary Policy

1. **Appendix 1: Privacy Notices**

Privacy Notice (How we use pupil information)

This Privacy Notice is designed to explain to pupils what data "The School" holds about them, how we use that data and who we share it with. This Notice was approved for publication on 15 May 2018 and is freely available on the school website.

The categories of pupil information that "The School" stores:

- Personal information
  - Full name, Date of birth, Unique pupil number, Exam candidate number, Address, Gender, School history, Photograph, CCTV images captured in school
- Parental information
  - Telephone numbers, Email addresses, Address, Relationship to pupil, Language
- Registration information
  - Registration group, Year group, Admission date, Admission number, Enrolment status
- Characteristics
  - Ethnicity, Language, Nationality, Country of birth, Free school meal eligibility, Religion, Transport method, Traveller status, Biometric details
- Medical information
  - Medical conditions, Medical Practice details, Medical events, Dietary requirements
- Special Educational Needs (SEN) and Disability information
  - SEN status, SEN reviews, Education Health Care Plan (EHCP) reviews, Reading age, Learning difficulties, Spelling age
- Attendance information
  - Percentage attendance, Sessions attended, Number of absences, Absence reasons
- Assessment information
  - Subjects studied, Timetable, Spotlight reports, Exam grades
- Behavioural information
  - Achievements, Behaviour incidents, Exclusions including reason and length of exclusion, Detentions including attendance record, Behaviour stage
- Careers information
  - Date of leaving, Reason for leaving, Destination upon leaving

Why we collect and use this information

We use pupil data:

to support pupil learning
to monitor and report on pupil progress
to provide appropriate pastoral care
to assess the quality of our services
to comply with the law regarding data sharing

The lawful basis on which we use this information

We collect and use pupil information under Article 6 of the General Data Protection Regulation (GDPR) because it is necessary for the performance of the school - it is in the public interest for the school to have all the information it needs to educate pupils effectively. Sometimes we collect and use extra pupil information and the school seeks the consent of the pupil (or their parent if the pupil is below the age of 13) in these instances. We also collect and use pupil information under Article 9 of the GDPR because it is in the public interest for us to do so.

Collecting pupil information

Whilst the majority of pupil information provided to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform pupils and parents/carers whether they are required to provide certain pupil information to us or if they have a choice in this.

Storing pupil data

We hold pupil data in the pupil file (paper and electronic) until the pupil has reached the age of 25. There are instances where the school holds onto certain data for longer. Please refer to the Data Protection Policy and the Data Retention Table that is included there for a full list of how long we store pupil data for.

Who we share pupil information with

We routinely share pupil information with:

- schools that the pupil attends after leaving us
- Bristol City Council
- the Department for Education (DfE)
- Independent Careers Service (NEWS)
- School Nurse
- Third-parties who provide educational resources and services (please contact the Data Protection Officer on dpo@holycross.bristol.sch.uk for a full list)

Why we share pupil information

We do not share information about our pupils with anyone without consent unless the law requires us to do so.

We share pupil data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education go to https://www.gov.uk/education/data-collection-and-censuses-for-schools

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law to provide information about our pupils to the DfE as part of statutory data collections such as the school census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.
To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website: https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold, known as a Subject Access Request (SAR). To make a SAR, or be given access to an educational record, we ask requesters to complete a SAR Form which is available on the school website or by contacting the Data Protection Officer by emailing dpo@holycross.bristol.sch.uk

Parents and pupils also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact

If you would like to discuss anything in this privacy notice, please contact the Data Protection Officer by emailing dpo@holycross.bristol.sch.uk

Privacy Notice for Parents / Carers

This Privacy Notice is designed to explain to parents and carers what data "The School" holds about them, how we use that data and who we share it with. This Notice was approved for publication on 15 May 2018 and is freely available on the school website.

The categories of information that "The School" stores:

- Personal information
  - Full name, Date of birth, Address, Gender, Telephone numbers, Email address, Address, Relationship to pupil, CCTV images captured in school
- Characteristics
  - Ethnicity, Language

Why we collect and use this information

We use pupil data:

to support pupil learning

to report on pupil progress

to provide appropriate pastoral care

The lawful basis on which we use this information

We collect and use information about parents/carers under Article 6 of the General Data Protection Regulation (GDPR) because it is necessary for the performance of the school - it is in the public interest for the school to have all the information it needs to educate pupils effectively and inform parents/carers about this education. Sometimes we collect and use extra information and the school seeks the consent of the parent/carer in these instances. We also collect and use pupil information under Article 9 of the GDPR because it is in the public interest for us to do so.

Collecting information

Whilst the majority of information provided to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform parents/carers whether they are required to provide certain information to us or if they have a choice in this.

Storing information

We hold information about parents/carers in the pupil file (paper and electronic) until the pupil has reached the age of 25. There are instances where the school holds onto certain data for longer. Please refer to the Data Protection Policy and the Data Retention Table that is included there for a full list of how long we store data for.

Who we share information with

We routinely share information about parents/carers with:

- schools that the pupil attends after leaving us
- Bristol City Council
- the Department for Education (DfE)
- Independent Careers Service (NEWS)

- Third-parties who provide educational resources and services (please contact the Data Protection Officer on dpo@holyycross.bristol.sch.uk for a full list)

Why we share information

We do not share information without consent unless the law requires us to do so.

We share pupil data (which includes information about parents/carers) with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Requesting access to your personal data

Under data protection legislation, parents/carers have the right to request access to information about them that we hold, known as a Subject Access Request (SAR). To make a SAR, or be given access to an educational record, we ask requesters to complete a SAR Form which is available on the school website or by contacting the Data Protection Officer by emailing dataprotection@stberns.bristol.sch.uk.

Parents/carers also have a legal right to access to their child's **educational record**. To request access, please contact the school office.

Parents/carers can make a request with respect to their child's data where the child is not able to understand their rights over their own data (usually under the age of 13), or where the child has provided written consent.

Parents/carers also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact

If you would like to discuss anything in this privacy notice, please contact the Data Protection Officer by emailing dataprotection@stberns.bristol.sch.uk.

Privacy Notice (How we use school workforce information)

This Privacy Notice is designed to explain to the school workforce what data "The School" holds about them, how we use that data and who we share it with. This Notice was approved for publication on 15 May 2018 and is freely available on the school website.

The categories of school workforce information that we collect, process, hold and share include:

- Personal information
    - Name, Address, Telephone number, Email address, National insurance number, Marital status, Disabilities, Staff identification code (initials), Sort code, Account number, Medical information, Dietary requirements, Car information, Next of kin details, Photograph, CCTV images captured in school
- Special categories of data including characteristics information
    - Gender, Age and date of birth, Ethnic group, Religion, Languages spoken, Nationality, Biometric details
- Contract information
    - Start date, Leaving date, Previous employer, Hours worked, Job title, Salary information, Payroll number, CPD record, DBS check information, Appraisal information, Lesson observation information
- Work absence information
    - Number of absences, Reasons for absence
- Qualifications
    - Subjects taught, QTS status

Why we collect and use this information

We use school workforce data 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

The lawful basis on which we process this information

We process this information under Article 6 of the GDPR as it is in the public interest that our workforce is effectively deployed to teach and support the education of our students and that staff welfare is considered to ensure students are taught in a happy and supportive environment. We also process information under Article 9 of the GDPR because it is in the public interest for us to operate effectively and with all available information at our disposal.

Collecting this information

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with data protection legislation, we will inform you whether you are required to provide certain school workforce information to us or if you have a choice in this.

Storing this information

We hold school workforce data for the length of employment at the school, plus six years. We will permanently keep a record of the employee's name, employment dates and job role for historical purposes.

Who we share this information with

We routinely share this information with:

- our local authority
- the Department for Education (DfE)
- third party suppliers who provide goods and services to the school

Why we share school workforce information

We do not share information about workforce members with anyone without consent unless the law and our policies allow us to do so.

Local authority

We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Department for Education (DfE)

We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment of educational attainment. We are required to share information about our school employees with our local authority (LA) and the Department for Education (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Third Party Suppliers

We share information with third party suppliers to ensure that appropriate access is given to any service they provide. We also share information so that they can effectively provide their service.

Data collection requirements

The DfE collects and processes personal data relating to those employed by schools. All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005.

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure that the confidentiality of personal

data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

To contact the department: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, we ask you to complete a Subject Access Request Form (SAR Form) from the school website. Further information can be obtained by contacting the Data Protection Officer by emailing dpo@holycross.bristol.sch.uk.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Further information

If you would like to discuss anything in this privacy notice, please contact the Data Protection Officer by emailing dpo@holycross.bristol.sch.uk.

- **Appendix 2: Data Retention Schedule**

Governing Body	
Data Item	**Retention Period**
Governing Body Agendas	Permanent
Governing Body Minutes	Permanent
Governing Body Minutes - Inspection Copies	3 years
Reports presented to the Governing Body	6 years
Instruments of Government including Articles of Association	Permanent
Trusts and Endowments managed by the Governing Body	Permanent
Action plans created and administered by the Governing Body	3 years
Policy documents created and administered by the Governing Body	3 years
Records relating to complaints dealt with by the Governing Body	6 years
Annual Reports created under the requirements of the Education Regulations 2002	10 years
Proposals concerning the change of status of a maintained school	3 years

Senior Leadership Team	
Data Item	**Retention Period**
Log books of activity maintained by the Headteacher	Minimum 6 years
Notes of SLT Meetings and other internal administrative bodies	3 years
Reports created by the Headteacher or other SLT members	3 years
Records created by the Headteacher, SLT, ACOs or other staff with administrative responsibilities	6 years
Correspondence created by the Headteacher, SLT, ACOs or other staff with administrative responsibilities	3 years
Professional Development Plans	6 years after completion
School Development Plans	3 years after completion

Admissions Process	
Data Item	**Retention Period**
All records relating to the creation and implementation of the School Admissions Policy	3 years
Successful admission	1 year after admission
Unsuccessful admission	1 year after resolution
Register of Admissions	Permanent

Casual Admissions	1 year
Proofs of address supplied by the parent	1 year
Supplementary Information Form - successful admission	Placed onto pupil file
Supplementary Information Form - unsuccessful admission	Resolution of appeal
Appeals Records	Resolution of appeal

Operational Administration	
Data Item	**Retention Period**
General file series	5 years
Records relating to the creation and publication of the school prospectus	3 years
Records relating to the creation and distribution to staff, parents and pupils	1 year
Newsletters	1 year
Visitor books and Signing in Sheets	6 years
Records relating to the creation and publication of the school prospectus	6 years

Recruitment	
Data Item	**Retention Period**
All records leading up to the appointment of a new Headteacher	6 years
All records leading up to the appointment of a new member of staff - unsuccessful candidate	6 months
All records leading up to the appointment of a new member of staff - successful candidate	Added to staff personal file
Pre-employment vetting information - DBS Checks	6 months
Proofs of identity collected as part of process of checking 'portable' enhanced DBS disclosure	Added to staff personal file
Pre-employment vetting information - Evidence proving the right to work in the UK	Added to staff personal file

Operational Staff Management	
Data Item	**Retention Period**
Staff Personal File	6 years after termination of employment
Timesheets	6 years
Annual appraisals	5 years

Disciplinary Process	
Data Item	**Retention Period**
Allegation of a child protection nature against a member of staff where the allegation is unfounded	Normal Retirement Age or 10 years, whichever is longer
Verbal Warning	6 months
First Written Warning	6 months
Final Warning	18 months
Case not found (not child protection)	Immediate

Health and Safety	
Data Item	**Retention Period**
Health and Safety Policy Statements	3 years
Health and Safety Risk Assessment	3 years
Records relating to an accident or injury at work	12 years
Accident Report - Adult	6 years
Accident Report - Child	Child turns 25
Control of Substances Hazardous to Health	40 years
Asbestos monitoring records	40 years
Radiation monitoring records	50 years
Fire Precaution log books	6 years

Payroll and Pensions	
Data Item	**Retention Period**
Maternity pay records	3 years
Records held under Retirement Benefits Scheme Regulations 1995	6 years

Risk and Asset Management	
Data Item	**Retention Period**
Employer's Liability Insurance Certificate	Closure of the School + 40 years
Inventories of furniture and equipment	6 years

Burglary, theft and vandalism reports	6 years

Finance	
Data Item	**Retention Period**
Annual Accounts	6 years
Loans and grants managed by the school	Last payment date + 12 years
All records relating to the creation and management of budgets	3 years
Invoices, receipts, order books and requisitions, delivery notices	6 years
Records relating to the collection and banking of monies	6 years
Records relating to the identification and collection of debt	6 years
School Fund - Cheque books	6 years
School Fund - Paying in books	6 years
School Fund - Ledger	6 years
School Fund - Invoices	6 years
School Fund - Receipts	6 years
School Fund - Bank statements	6 years
School Fund - Journey Books	6 years
All records relating to the management of contracts under seal	Last payment date + 12 years
All records relating to the management of contracts under signature	Last payment date + 6 years
Records relating to the monitoring of contracts	2 years
Free School Meals Registers	6 years
School Meals Registers	3 years
School Meals Summary Sheets	3 years

Property Management	
Data Item	**Retention Period**
Title deeds of properties belonging to the school	Permanent

Plans of property belonging to the school	Permanently whilst owned by the school
Leases of property leased by or to the school	6 years
Records relating to the letting of school premises	6 years
All records relating to the maintenance of the school carried out by contractors	6 years
All records relating to the maintenance of the school carried out by school employees including maintenance log books	6 years

Pupil Management	
Data Item	**Retention Period**
Pupil's Educational Record (ie Pupil File)	Until pupil is 25
Examination Results (Public)	Permanent (Register of Admissions)
Examination Results (Internal Exams)	Until pupil is 25
Child Protection information held on the pupil file.	Until pupil is 25
Child Protection information held in separate files.	Until pupil is 25
Attendance Registers	Until pupil is 25
Correspondence relating to authorised absence	2 years
Special Educational Needs files, reviews and Individual Action Plans	Until pupil is 25
Statement maintained under section 234 of the Education Act 1990 and any subsequent amendments	Until pupil is 25
Advice and information provided to parents regarding educational needs	Until pupil is 25
Accessibility Strategy	Until pupil is 25

Curriculum Management	
Data Item	**Retention Period**
Curriculum Returns	3 years
Examination Results	Permanent
Examination Papers	Until any appeal process is complete

Published Admission Number (PAN) Reports	6 years
Value Added and Contextual Data	6 years
Self Evaluation Forms	6 years
Schemes of Work	1 year
Timetables	1 year
Class Record Books	1 year
Mark Books	1 year
Record of homework set	1 year
Pupil Work	1 year

Extra-Curricular Activities	
Data Item	**Retention Period**
Records created to obtain approval to run an Educational Visit outside the Classroom	Date of Visit + 10 years
Parental consent forms for school trips where there has been no major incident	Conclusion of visit
Parental consent forms for school trips where there has been a major incident	DOB of the pupil involved + 25 years
Walking Bus Registers	3 years

Family Liaison Officers and Home School Liaison Assistants	
Data Item	**Retention Period**
Day Books	2 years
Reports for outside agencies	When child leaves the school
Referral forms	Until referral is closed
Contact data sheets	End of academic year
Contact database entries	End of academic year
Group Registers	2 years

Central Government and Local Authority

Data Item	Retention Period
Secondary Transfer Sheets	2 years
Attendance Returns	1 year
School Census Returns	5 years
Circulars and other information sent from the Local Authority	Operational use
OFSTED Reports and papers	Life of the report
Returns made to central government	6 years
Circulars and other information sent from the central government	Operational use

•

- **Appendix 3: Subject Access Request Form**

Please write in BLACK in BLOCK CAPITAL LETTERS inside the boxes.

I am the Data Subject (The person the information is about): ☐

OR

I am acting on behalf of the Data Subject: ☐

Note: If you are seeking information on behalf of someone who is unable to act for themselves, you must explain your relationship, what information you require and why it is required. Please note that information relating to someone else will not be disclosed without the data subject's written consent or an appropriate Court Order or Power of Attorney. Accordingly I enclose:

The Data Subject's written consent to disclosure of the information requested at Part 2:	☐
A Court Order permitting release of the information requested at Part 2:	☐
My relationship to the data subject is: (Please specify e.g. Doctor/Solicitor/Spouse/Civil Partner/Parent/Sibling)	

Part 1: Data Subject Personal Details

Surname		Forename(s)		Title	
Date of Birth		Email Address			
Address			Telephone Number		
Please explain your relationship with the school (e.g. past pupil, former staff member)					
Dates attended or worked at "The School"					

Please provide the address you would like the information sent to. If you are completing this form on behalf of someone else, please complete this section too.

Surname		Forename(s)		Title	
Email Address					

Address		Telephone Number	

Part 2: Information Requested

Please state details about the information you are requesting. Please be as detailed as you can, and where possible, include dates.
For example: I would like to have details from my behaviour record when I attended the school between 2005 and 2009.

"The School" will use the information provided to locate the data sought. Your request will be processed in accordance with the General Data Protection Regulation.

Part 4 – Declaration by Requestor

Name in Capitals:
Signature:
Date:

Verification of identity is required before your request can be processed

I enclose as verification of identity a copy of my	Passport ☐	Driving Licence ☐	Utility Bill ☐	Other ☐

I declare that, to the best of my knowledge, the information I have provided on this form is correct			
Signature		Print Name	
		Date	

- **Appendix 4: Right to Be Forgotten Form**

Important: Proof of identity (e.g. drivers licence, passport) must accompany this form.

Full Name	
Address	
Contact number *	Email addresses *

* The school may need to contact you to discuss your request.

Please tick the box which applies to you:

Student ☐	Parent/Carer of student ☐	Former Student ☐	Current Staff ☐	Former Staff ☐
Age: Year group: House:	Name of Student:	Year of leaving:		Years From/To:

I, _____[insert name] wish to have the data detailed below which "The School" holds about me erased. I am making this request under Article 17 of the General Data Protection Regulation.

Details of the information you wish to have erased:

Please note that your right to request erasure is not absolute and may be declined by "The School" in certain cases. The School will fully explain this to you if this is the case.

Signed _____ Date _____

Please return this form to: **Data Protection Officer, at School**

- **Appendix 6: Personal data breach procedure**

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the Headteacher and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss

- Unauthorised reversal of pseudonymisation (for example, key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's computer system.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours of the breach being reported. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects

- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on the school's computer system. The DPO, Headteacher and other relevant staff will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, the DPO will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Non-anonymised pupil exam results or staff pay information being shared with governors

- Governors should receive anonymized information about pupil exam results and staff pay information. The DPO must be informed by the meeting convenor as soon as possible about non-anonymised information being shared with governors
- Governors will be asked to return their papers by the meeting convenor. They will be issued anonymized papers in their place
- Should any governor be unavailable or not present at the meeting, the DPO will contact these governors and request the papers be destroyed by the governor. The governor will be asked for written confirmation that this has taken place
- Any papers that were sent electronically will need to be deleted by governors. The DPO will ask for written confirmation that these emails and files have been permanently deleted
- The DPO will carry out an internet search to check that the information has not been made public; if it has, the DPO will contact the publisher/website owner or

administrator to request that the information is removed from their website and deleted

A portable school device containing non-encrypted sensitive personal data being lost, stolen or hacked

- For non-encrypted devices, the DPO will request a summary of the files that were being stored on the device and a list of the sensitive personal data that was being stored on the device
- Where possible, the DPO will contact those people who have had their sensitive personal data lost, stolen or hacked and explain the incident to them
- The theft or hack of a device will be reported to the police by the DPO. Lost devices will also be registered with the police
- The DPO will carry out internet searches to check that the information has not been made public; if it has, the DPO will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

- **Appendix 7: data breach**

1. Defining 'personal data'

a. The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. e.g. name, identification number, location data, photo, or online identifier.
b. Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.
c. The GDPR refers to sensitive personal data as "special categories of personal data" - genetic data, and biometric data where processes can uniquely identify an individual.

2. Defining a data breach

a. A 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

3. Who should I tell?

a. If you know of or suspect a data breach you should immediately contact the Data Protection Officer who is the Business Manager. In their absence the Head Teacher must be informed.

4. The Head Teachers role

a. The Head Teacher will require the Data Protection Officer to investigate any breach, take whatever recovery actions as may be appropriate, notify subjects and ICO in the event of a breach, and make any changes to practices, policies and or procedures as is necessary to prevent reoccurrence.
b. In the absence of the Data Protection Officer, the Head Teacher will appoint a Deputy Data Protection Officer to fulfil the immediate demands of the Data Protection Officer role.

5. Data Protection Officer's role

The data protection officer will:

a. Notify the Head Teacher;
b. Investigate the matter to determine whether there has been a breach or near miss;
c. Take immediate action to recover data where possible;
d. Notify the data subjects as to what data has been disclosed, to whom and how, and to inform them of actions taken to remedy the breach, and advise them of their right to register a complaint with the ICO (helpline 0303 123 1113);
e. Notify the Information Commissioner's Office of the breach and actions taken;
f. Notify the Chair of Governors;
g. Keep a record of all actions and when taken.

6. Reporting a data breach

a. Notification to Data Subjects

The DPO will communicate with the data subjects of a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority,

respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities.

b. Notification to the ICO.
The GDPR introduces a duty on all organisations to report certain types of personal data breach to the ICO. You must do this within 72 hours of becoming aware of the breach, where feasible.

The ICO can be contacted at:
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Tel: 0303 123 1113 (local rate) or 01625 545 745 Further guidance and documentation can be found at:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

7. Remedial processes

a. If a breach has occurred the Data Protection Officer will investigate to see whether the breach can be mitigated by, for example, freezing email accounts or retrieving the data.

b. Data subjects should be given information and recommendations about what actions they can take to protect themselves and to limit the damage caused by the breach. This may involve discussion with the ICO to obtain their advice first.

8. Post implementation review

a. After all the above actions have been taken the Data Protection Officer will review as appropriate the schools processes, systems and training in order to improve the data security. They will, if required, draw up an action plan with time lines and clear responsibilities which they will share with the Audit Committee until all actions are completed or struck out as no longer necessary.