



**Personal Data Handling Policy**  
**Written May 2018 – Review date October 2024**

**1.0 Aims**

- 1.1 Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.
- 1.2 This policy applies to all personal data, regardless of whether it is in paper or electronic format.

**2.0 Policy Statement**

- 2.1 Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.
- 2.2 Our school will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- 2.3 Every effort will be made to ensure that data held is accurate and up to date. Individuals have the right to have personal data rectified where the records held are inaccurate or incomplete. Where we have held and processed incorrect data involving a third party e.g. an exam board or the school nurse, we will ensure that they receive corrected information. All actions to rectify information held by BCS and forwarded to 3<sup>rd</sup> parties will be completed within 1 month of receipt of the new information.
- 2.3 All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in a transparent manner. All personal data will be processed and stored with appropriate security including protection against unlawful or unauthorised processing and against accidental loss, destruction or damage using appropriate technical and organisational measures.
- 2.4 Individuals have the right to access their personal data and the right to verify the lawfulness of the processing. Please see section 10 for information on Subject Access Requests.
- 2.5 An individual is able to request deletion or removal of personal data where there is no compelling reason for its continued retention. The right to erasure does not apply where the information is still being used to comply with a legal obligation.

**3.0 Personal Data**

- 3.1 Certain staff in the school will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records.
- 3.2 Personal data is defined as any information relating to an individual person who can be directly or indirectly identified in particular by reference to an identifier. This will include:
- Personal information about members of the school community – including students, members of staff and parents / carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
  - Curricular / academic data e.g. class lists, student progress records, reports, references
  - Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
  - Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members. E.G. Payment records / financial records.
  - Personal information that may be shared with the Charities Commission.

**4.0 Responsibilities**

- 4.1 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 board and, where relevant, report to the board 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.
- 4.2 Our DPO is Zeilah Chadwick and is contactable at [mrschadwick@bxs.org.uk](mailto:mrschadwick@bxs.org.uk)
- 4.3 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 UK
- 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

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

## 5.0 **Registration**

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner; registration number Z5277563

## 6.0 **The Privacy Notice**

### 6.1 **Information to Parents / Carers**

In order to comply with the fair processing requirements UK GDPR, the school will inform parents / carers of all students of the data they collect, process and hold on the students, the purposes for which the data is held and the third parties (e.g. school nurse, exam boards, etc) to whom it may be passed. This privacy notice will be passed to parents / carers via the MIS system on an annual basis and will be available on the school website. The notice to be used by the school is at Annex A to this policy and will be sent out annually to all parents and carers via MIS. As explained in the privacy notice, the data that BCS processes is necessary for compliance with legal obligations to which the controller is subject.

### 6.2 **Staff, Volunteers and Governors**

Personal information is also held for staff, volunteers and governors, as employer the school will annually provide a privacy notice to all staff, volunteers and governors informing them of the data we collect and process and the purpose for which that data is held and any third parties to whom it may be passed. The notice to be used by the school is at Annex B to this policy and will be sent out annually to all staff in October via MIS each year and will be available on the school webpage

## 7.0 **Training & Awareness**

7.1 All staff will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- Staff meetings / briefings / Inset
- Day to day support and guidance from the school business manager and Mr McGrail.

## 8.0 **Information Asset Audit**

8.1 BCS has completed an Information Asset Audit which identifies all personal Information that is held on individuals indicating:-

- Where it came from
- Who we share it with

8.2 BCS has created a data asset register detailing :

- How the information is stored and ensure that it is stored safely and securely.
- Any concerns and their resolution
- Retention and destruction
- Processing completed with the data

## 9.0 **Secure Storage of; and Access to Data**

BCS ensures that systems have been set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user.

- 9.1 All users will use strong passwords (see the Bradford Christian School Technical Security Policy and Online safety policy re password security) User passwords will never be shared.
- 9.2 Personal data will only be accessed on machines that are securely password protected. Any device that can be used to access data will be locked if left (even for very short periods) and set to auto lock if not used for five minutes.
- 9.3 All storage media will be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

**Personal data should be stored by users of school equipment on the cloud rather than removable media except in circumstances agreed by SLT. Where removable media is used (e.g. memory sticks / CDs / DVDs) they must be encrypted and stored securely in school and should not be removed from school unless permission is expressly given by SLT.**

**Private equipment (i.e. owned by the users) must not be used for the storage of personal data.**

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected,
  - the device must be password protected
  - the device must offer approved virus and malware checking software
  - the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.
- 9.4 Unless otherwise directed, staff will be expected to store any documents containing personal data on BCS drive and each member of staff has access to store data securely in this area.
- 9.5 BCS has clear policy and procedures for the use of “Cloud Based Storage Systems” (see 9.4) (for example google apps and google docs) and is aware that data held in remote and cloud storage is still required to be protected in line with UK GDPR. BCS will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.
- 9.6 As a Data Controller, BCS is responsible for the security of any data passed to a “third party”. Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.
- 9.7 **All paper based material containing personal data will be held in lockable storage.**

## 10.0 Subject Access Requests

10.1 “a data subject **has** the right of access to personal data which **has** been collected concerning **them**, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing.”

10.2 In compliance with this regulation, if you wish to see a copy of the information held in relation to yourself or your child please email or write to the school office stating what information you wish to see a copy of and in relation to whom. The school business manager will:-

- Respond to your request within one month unless the request is complex or numerous, in which circumstance BCS is permitted to extend the deadline to three months. However, BCS will still respond to the request within a month to explain why the extension is necessary.
- Provide the information free of charge unless a request is manifestly unfounded, excessive or repetitive then a fee will be charged based on the administrative cost of providing the information.
- Provide a description of the data held
- Explain the purpose for which the data is processed
- Disclose the sources of that data and to whom the data may be disclosed;
- Provide a copy of all the personal data that is held about the individual redacting any data that is about another person.

## 11.0 Secure Transfer of Data and Access Out of School

The school recognises that personal data may be accessed by users out of school, or transferred to exam boards or other agencies. In these circumstances:

- Users may not remove or copy sensitive personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school.

- When restricted or protected personal data is required by an authorised user from outside the organisation’s premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform.
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location
- In accordance with the technical security policy, only portable and mobile devices purchased by the school and appropriately encrypted can be used to store and transmit personal data where use of the cloud is not possible.
- Data stored is only permissible to be transferred within the European Economic Area where appropriate, and transfer of data beyond that area would be classed as a breach of UK GDPR rules.

## 12.0 **Disposal of Data**

The school will comply with the requirements for the safe destruction of personal data when it is no longer required. As a guide the destruction of data will follow the schedule at Annex E

- 12.1 The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance and other media must be shredded, incinerated or otherwise disintegrated.
- 12.2 A Destruction Log (Annex C) will be kept of all data that is disposed of. The log should include the document ID, date of destruction, method and authorisation.

## 13.0 **Personal Data Breaches**

13.1 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. This includes breaches that are the result of both accidental and deliberate causes. Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

13.2 When a security incident takes place, we will quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required. When a personal data breach has occurred, BCS will establish the likelihood and severity of the resulting risk to people’s rights and freedoms. If it’s likely that there will be a risk then BCS will notify the ICO within 72 hours. Where BCS decides not to report the breach, we will document the reasons why.

13.3 If a breach is likely to result in a high risk to the rights and freedoms of individuals, BCS will inform those concerned directly as soon as possible.

13.4 Where possible BCS documents the activities where possible of data users in our electronic environment using electronic logs. These logs will be monitored by Mr Shaun McGrail

13.5 The audit logs will be kept to provide evidence of accidental or deliberate data security breaches – including loss of protected data or breaches of an acceptable use policy, for example; the school has a system for reporting, managing and recovering from information risk incidents, which establishes:

- a “responsible person” for each incident
- a communications plan, including escalation procedures
- a plan of action for rapid resolution and
- a plan of action of non-recurrence and further awareness raising.

13.6 BCS will record all personal data breaches (Annex D), regardless of whether or not they need to be reported to the ICO and document the facts relating to the breach, its effects and the remedial action taken. The log will record whether or not the breach was a result of human error or a systemic issue and establish how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps.

## 14.0 **Data Sharing**

14.1 Wherever BCS (the data controller) shares data with a third party (a data processor) for example and exam board for GCSE examinations, **BMDC for EYFS funding**, **Integrated front door for safeguarding concerns** or the school nurse, we will ensure that a written contract is in place to ensure that both parties understand their responsibilities and liabilities in relation to the personal data that has been shared.

14.2 These contracts will contain:-

- the subject matter and duration of the processing
- the nature and purpose of the processing
- the type of personal data and categories of data subject
- The obligations and rights of the controller
- That the data processor must only act on the written instruction of the data controller
- That the data processor must ensure that the people processing the data are subject to a duty of confidence
- That the data processor takes appropriate measures to ensure the security of processing

#### 15.0 **Privacy and Electronic Communications**

15.1 BCS complies with UK GDPR and the Privacy and Electronic Communications Regulations in the operation of their websites and electronic communications including texts, e-mail and social media, covering all advertising or promotional details including promoting the aims or ideals of the school to those who do not currently have a child or work in the school.

15.2 We will actively seek to gain consent from all recipients on our mailing lists. We will retain clear records of the consent received and will ensure that the party has the opportunity to withdraw consent at any time.

#### 16.0 **Freedom of Information**

16.1 BCS proactively publishes information and policies on the school web page.

16.2 Where information of a general nature in relation to school policies is not available on the web page; a request can be made to the school business manager for the required information. The school business manager will prepare a response in consultation with the head teacher and chair of governors.

16.3 Where a request for information is refused a record of refusals and reasons for refusals will be kept.

#### 17.0 **CCTV Usage**

17.1 Bradford Christian School uses Close Circuit Television (CCTV) within the premises of the School. The system comprises a number of internal and external day and night cameras and does not use any sound recording capability. The CCTV system is owned and operated by the School, the use of which is directed by the Senior Leadership Team.

17.2 Access and viewing is restricted and authorised operators with access to images will be aware of the procedures they are required to follow and the restrictions in relation to access to, and disclosure of, recorded images.

17.3 The School uses CCTV for the following purposes:

- To provide a safe and secure environment for pupils, staff and visitors;
- To protect the school buildings and assets;
- To assist in reducing the fear of crime and for the protection of private property;
- To assist in the prevention of crime and assist law enforcement agencies in apprehending offenders,
- To monitor activities within the school grounds to identify potential criminals,
- To monitor activity for the purpose of securing the safety and well-being of the school,
- To monitor student behaviour

The school will not direct cameras outside of the school site at private property, an individual, their property or at a specific group of individuals.


17.4 The school will:

- notify the Information Commissioners Office of its use of CCTV as part of the annual data protection registration; and will treat the system and all information processed on the CCTV system as data which is covered by the Data Protection Act/UK GDPR;
- display CCTV warning signs on the building indicating that the premises are protected by CCTV and that recording is taking place.

- release recorded materials for the use in the investigation of a specific crime and with the written authority of the Police and in accordance with the Data Protection Act/UK GDPR.
- 17.5 Cameras will be sited so they only capture images relevant to the purposes for which they are installed and care will be taken to ensure that reasonable privacy expectations are not violated. For example, cameras will not be placed in areas which are reasonably expected to be private such as in toilets or changing areas.
- 17.6 Recorded data will not be retained for longer than is necessary. All retained data will be stored securely and kept for 29 days on a secure central server.
- 17.7 Any Individual recorded in any CCTV image is a data subject for the purposes of the Data Protection Legislation, and has the right to request access to those images. Such a request will be processed in the context of a Subject Access Request. Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. For example, date, time and location. The school reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation.
- 17.8 The ability to view live and historical CCTV data available via network software is provided in the school office and to authorised persons only.
- 17.9 Data from CCTV may be used within the school’s safeguarding procedures as required.

**18.0 Development / Monitoring / Review of this Policy**

- 18.1 This Data handling policy has been developed in consultation with:
- Headteacher and Senior Leadership Team
  - Online Safety Officer
  - Staff – including Teachers, Support Staff
  - Governors
- 18.2 In writing this policy Bradford Christian school acknowledges:
- the materials supplied and used from SWGfL Online Safety School Template Policies
  - UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
  - ICO’s video surveillance (including guidance for organisations using CCTV).
  - Guide to General data protection regulations
  - Data protection: a toolkit for schools
  - Data Protection Act 2018
- 18.3 This policy should be read in conjunction with the following school policies:
- Technical security policy
  - On Line safety policy
  - Behaviour and Discipline Policy (students)
  - Discipline Policy (staff)
  - Safeguarding and child protection policy
  - Preventing extremism and radicalisation policy
  - Safer recruitment policy
  - Staff code of conduct
- 18.4 This policy was first written in May 2018 and will be reviewed annually, this latest review being completed in September 2023

Formally agreed through Governors compliance:	<b>5<sup>th</sup> October 2023</b>
Signed Richard Shackleton – Chair of Governors	
Signed Jane Prothero – Head Teacher	
Review Date:	<b>October 2024</b>



## Privacy Notice – How we collect and use pupil information

Written May 2018 – Review date October 2024

### 1.0 Privacy Notice (How we use pupil information)

1.1 This notice is to give pupils and parents insight into how information about pupils and families is used in Bradford Christian School

1.2 The categories of pupil information that we collect, hold and share include:

- Personal information (such as name, unique pupil number and address) *this is a legal obligation under the Education(pupil registration)(England) Regulations 2006*
- Attendance information (such as sessions attended, number of absences and absence reasons) *this is a legal obligation under the Education(pupil registration)(England) regulations 2006*
- Assessment information *this is a legal obligation under the Education (Pupil Information)(England) Regulations 2005*
- Relevant medical information, *this is a legal obligation under Section 100 of the Children and Families Act 2014 which places a duty on governing bodies of maintained schools, proprietors of academies and management committees of PRUs to make arrangements for supporting pupils at their school with medical conditions.*
- Special educational needs information, *this is a legal obligation under the Education (Pupil Information)(England) Regulations 2005*
- Exclusions / behavioural information, - *this is an Ofsted requirement*
- Safeguarding – *this is a legal obligation under Keeping children safe in education and also the Education (Independent School Standards) Regulations April 2019*

### 2.0 Why we collect and use this information

2.1 We use the 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
- **to comply with the EYFS (Statutory Framework) 3.69 'Providers must maintain records and obtain and share information (with parents and carers, other professionals working with the child, the police, social services and ISI to ensure the safe and efficient management of the setting, and to help ensure the needs of all children are met'**
- **Data collected via the Early Years Funding Parent Agreement Form will be shared with Bradford Metropolitan District Council (BMDC) for the purpose of checking eligibility and securing funding. We will retain the Early Years Funding Parent Agreement Form for a period of 4 years from the child's start date, to enable Bradford Council to carry out compliance visits, audits and if necessary fraud investigations.**
- **Bradford Metropolitan District Council will collect and retain information submitted by the school provider to administer the early years funding, and for auditing purposes. BMDC collects some or all of the following information from funded providers about children and their parents who are accessing funded entitlements:**
  - **Personal information of the child** as set out in the Early Years Funding Parent Agreement: Full name (as stated on birth certificate), Date of birth, Address, Gender, Ethnicity, Language, Number of entitlement hours they are accessing, Details of other provider/s the child attended including start and end date.
  - **Personal information of the parent** as set out in the Early Years Funding Parent Agreement: Name, Address, Date of birth, Contact details, National insurance number, National Asylum Seeker's Support Number, HMRC 30-hour eligibility code, Eligibility for Early Years Pupil Premium, Eligibility for Disability Access Fund

### 3.0 The lawful basis on which we use this information

3.1 We collect and use pupil information under Article 6 where processing is necessary for compliance with a legal obligation to which the controller is subject.

3.2 We collect and use sensitive pupil health information under Article 9 (h) where processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of State law

#### **4.0 Collecting pupil information**

4.1 Whilst the majority of pupil information you provide 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 you whether you are required to provide certain pupil information to us or if you have a choice in this.

#### **5.0 Storing pupil data**

5.1 We hold pupil data for the length of time that the student is a pupil in the school and will destroy data in line with the data retention document that can be viewed within the data protection policy.

#### **6.0 Who we share pupil information with**

6.1 We routinely share pupil information with:

- schools that the pupil's attend after leaving us
- our local authority
- school nurse
- NHS
- Examination bodies
- **Independent Schools Inspector (ISI)**
- **Bradford safeguarding partnership – the integrated front door (IFD) & safeguarding professionals**

#### **7.0 Why we share pupil information**

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

#### **8.0 Youth support services Pupils aged 13+**

8.1 Once our pupils reach the age of 13, we also pass pupil information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

8.2 This enables them to provide services as follows:

- youth support services
- careers advisers

8.3 A parent or guardian can request that **only** their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the child once he/she reaches the age 16.

8.4 For more information about services for young people, please visit our local authority website.

#### **9.0 Requesting access to your personal data**

9.1 Under data protection legislation, parents and pupils have the right to request access to information about them that BCS holds. To make a request for your personal information, or be given access to your child's educational record, contact Mrs Zeilah Chadwick the School Business Manager.

9.2 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;
- claim compensation for damages caused by a breach of the Data Protection regulations

9.3 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/>

#### **10.0 Contact**

10.1 If you would like to discuss anything in this privacy notice, please contact:

Mrs Zeilah Chadwick School Business Manager, Bradford Christian school, Livingstone Road, Bradford, BD2 1BT.





**Privacy Notice – How we collect and use staff/governor information**

**Written May 2018 – Review date October 2024**

**1.0 Privacy Notice (How we use staff, volunteer and governor information)**

1.1 This notice is to give staff, volunteers and governors insight into how information about them is collected and used in Bradford Christian School

1.2 The information we collect, hold and share includes:

- personal information such as your name, address and contact details, including email address and telephone number, date of birth, gender and teacher number;
- the terms and conditions of your employment;
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with Bradford Christian School
- information about your remuneration, including entitlement to benefits such as pensions
- details of your bank account and national insurance number;
- information about your marital status, next of kin, dependants and emergency contacts;
- information about your nationality and entitlement to work in the UK;
- information about your criminal record;
- details of your schedule (days of work and working hours) and attendance at work;
- details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave;
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence;
- assessments of your performance, including appraisals, performance reviews and ratings, performance improvement plans and related correspondence;
- information about medical or health conditions, including whether you have a disability for which the organisation needs to make reasonable adjustments.

1.5 Data will be stored in a range of different places, including in your personnel file, your absence management file, the single central register, and in other IT systems including the organisation's email system.

**2.0 Why we collect and use this information**

2.1 BCS needs to process data to enter into an employment contract with you and to meet its obligations under your employment contract. For example, we need to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer pension entitlements.

2.2 In some cases, BCS needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled.

2.3 In other cases, the organisation has a legitimate interest in processing personal data before, during and after the end of the employment relationship. Processing employee data allows the organisation to:

- run recruitment processes
- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights
- Maintain the Single Central Register
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace
- operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes;
- operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled

- obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled;
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the organisation complies with duties in relation to leave entitlement
- to ensure that employees are receiving the pay or other benefits to which they are entitled;
- ensure effective general HR and business administration;
- provide references on request for current or former employees;
- respond to and defend against legal claims.
- Some special categories of personal data, such as information about health or medical conditions, is processed to carry out employment law obligations (such as those in relation to employees with disabilities)

### 3.0 **The lawful basis on which we process this information**

3.1 We process staff data under The general data protection regulation Article 6 where:

- processing is necessary for compliance with a legal obligation to which the controller is subject
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

3.2 We also process data under The general data protection regulation Article 9(2) where processing is necessary for the purpose of assessment of the working capacity of the employee

### 4.0 **Collecting this information**

4.1 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.

4.2 BCS collects this information in a variety of ways, E.G. through application forms, obtained from your passport or other identity documents such as your driving licence; from forms completed by you at the start of or during employment; from correspondence with you; or through interviews, meetings or other assessments.

4.3 BCS will also collect personal data about you from third parties, such as references supplied by former employers, and information from criminal records checks permitted by law.

### 5.0 **Storing this information**

5.1 We hold school workforce data for the length of time that the individual is officially connected to the school and will destroy data in line with the data retention document that can be viewed within the data protection policy.

5.2 Data will be stored in a range of different places, including in your personnel file, your absence management file, the single central register, and in other IT systems including the organisation's email system.

### 6.0 **Who we share this information with/ has access to this information:**

6.1 We routinely share this information with:

- our local authority
- the Department for Education (DfE)
- HMRC
- The school pension provider

6.2 We do not share information about staff with anyone without consent unless the law and our policies allow us to do so. E.G.

- Department for Education (DfE). We share personal data with the Department for Education (DfE) on a statutory basis.
- Your information may be shared internally, including the school business manager and school secretary for payroll, your line manager, other SLT managers as appropriate and IT staff if access to the data is necessary for performance of their roles.
- BCS shares your data with third parties in order to obtain pre-employment references from other employers and obtain necessary criminal records checks from the Disclosure and Barring Service.

- BCS shares your data with third parties that process data on its behalf, in connection with payroll, and the provision of benefits.

## 7.0 **Requesting access to your personal data**

7.1 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, contact the school business manager

7.2 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

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

## 8.0 **Further information**

8.1 If you would like to discuss anything in this privacy notice, please contact: Mrs Zeilah Chadwick School Business Manager, Bradford Christian school, Livingstone Road, Bradford, BD2 1BT.

**Bradford Christian School – Data Destruction Log**

<b>Document ID</b>	<b>Date of Destruction</b>	<b>Method</b>	<b>Authorisation</b>

**Personal Data Breaches**

**Annex D**

Date	Description of Breach	Human Error/ Systemic Error	Resolution	Plan to Prevent Reoccurrence	Report to ICO Yes/No + Reason	Report to Individual Yes/No + Reason

Destruction Schedule for Documents Holding Personal Data

Data Item	Duration to be Held For	Justification
Admissions	+ 1 year after subject has left school	Information used to validate and cross check enrolment details
Admissions (unsuccessful)	+ 3 months after initial contact	Information retained for appeal or if further application made  A list of names and reason for rejection will be retained for 2 years but no other data
Attainment	+ 3 years after subject has left school	Important for future schools to understand previous attainment and allows for handover.  After 2 years look to remove identifying data e.g. name date of birth, but retain outcomes for trend analysis
Attendance	+ 3 years after subject has left school	Important for future schools to understand previous attendance and allows for handover
Accident records	+ 6 years after the last entry was made	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) (SI 1995/3163) as amended.
Behaviour Records	+ 1 year after subject has left school	Important for future schools to understand previous behaviours and allows for handover
Exclusions	+ 1 year after subject has left school	Important for future schools to understand previous behaviours and allows for handover
EYFS Funding forms	+4 years from child's start date	To obtain LEA funding for EYFS education fees
eyLog Forms	When student leaves EYFS	To give access to students work
Trips and activities (permission slips)	One term after trip	
Educational Trip Risk Assessments	+ 6 years from the date of the trip	
Medical Information (Annual form pupil)	For 1 Year	Medical information is updated annually with parents and previous forms should be destroyed as new information is received.
Medicine Administration (pupil)	For 6 years	
Safeguarding	Until pupil is aged 25 if we are the last educational establishment	All safeguarding files should be transferred in their entirety to the next educational establishment unless there is no further educational establishment in which case apply the retention policy
Special educational needs	+ 1 year after subject has left school	Important for future schools to understand previous needs and allows for handover
Images used in school displays	Destroyed once a child leaves the school	Can be retained whilst the child is in school in line with parental consent

		To use images after a child has left school requires informed consent and the opportunity to request images to be removed
Names, Addresses and Date of Birth of pupils	+ 3 years after subject has left school	To enable references to be completed as required.
Photographic images	Should be deleted when a child leaves the setting	Unless specific consent has been given to continue using an image e.g. in promotion literature
Staff maternity records	+6 years after the end of the tax year in which the maternity period ends	The Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960) as amended
Wage and salary record	+ 6 years from the date paid	The Income Tax (Employments) Regulations 1993 (SI 1993/744) as amended, for example by The Income Tax (Employments) (Amendment No. 6) Regulations 1996 (SI 1996/2631) Taxes Management Act 1970
Application forms and interview records for unsuccessful candidates	+ 1 year from the end of the campaign	This period takes into account the fact that a job applicant can bring a claim for discrimination in the Employment Tribunal within 3 months from the date of the rejection for the role
Staff /volunteer / governor personnel files	+6 years after employment ceases	The Limitations Act 1980 (to reflect that legal proceedings must start within 6 years)
Staff sick records	+6 years after the end of the tax year to which they relate	The Statutory Sick Pay (General) Regulations 1982 (SI 1982/894) as amended
Learning Walks	+1 year from date completed	
Staff Appraisals	+3 years from the date completed	
Payment records / financial records in relation to parents.	+6 years from the end of the last company financial year they relate to	UK Tax laws
Information shared with charities commission	+6 years from the end of the last company financial year they relate to	
Visitors Books	+6 years from the date of the last entry	D of E guidance