

Date: August 2023  
Review date: August 2025  
Responsibility: DR

# Bishop Challoner School



## Data Protection Policy



## Bishop Challoner School Data Protection Policy

Relevant Acts: General Data Protection Regulations (GDPR) 2018

Data Protection Act 2018

Protection of Freedoms Act 2012

Education Act 2011

This policy should be read in conjunction with:

CCTV Policy

Information Security Policy

Retention Policy

Privacy Notice

Bishop Challoner School collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

In this policy, Bishop Challoner is the “Data Controller” and its employees, customers, suppliers, contractors and other business contacts are the “Data Subjects”.

### **Purpose**

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 2018 and General Data Protection Regulations (GDPR) 2018, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

### **The Data Protection Principles**

This Policy aims to ensure compliance with the Act. The Act sets out eight principles with which any party handling personal data must comply. All personal data:

- Must be processed fairly and lawfully (and shall not be processed unless certain conditions are met)
- Must be obtained only for specified and lawful purposes and shall not be processed in any manner which is incompatible with those purposes
- Must be adequate, relevant and not excessive with respect to the purposes for which it is processed
- Must be accurate and, where appropriate, kept up-to-date

- Must be kept for no longer than is necessary in light of the purpose(s) for which it is processed
- Must be processed in accordance with the rights of data subjects under the Act
- Must be protected against unauthorised or unlawful processing, accidental loss, destruction or damage through appropriate technical and organisational measures
- Must not be transferred to a country or territory outside of the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

### **Rights of Data Subjects**

Under the Act, data subjects have the following rights:

- The right to be informed that their personal data is being processed
- The right to access any of their personal data held by the school within 30 days of making a request
- The right to prevent the processing of their personal data in limited circumstances
- The right to rectify, block, erase or destroy incorrect personal data.
- The right to complain to the Information Commissioner's Office (ICO)

### **What is Personal Information?**

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held. Personal data includes information necessary for employment and may include:

- Pupil names, contact details, next-of-kin, birth dates, attendance records;
- Reports or grades, appraisals etc.;
- Sensitive personal data such as medical conditions, ethnic groups, or criminal records and proceedings and in relation to parents and/or guardians, financial information; and
- Images of staff and pupils engaging in school activities.

Personal data will usually be collected directly from you, but some may be passed to the school by third parties (e.g. other schools).

The Act further defines "sensitive personal data" as personal data relating to:

- The racial or ethnic origin of the data subject
- Their political opinions
- Their religious (or similar) beliefs
- Trade union membership
- Their physical or mental health condition
- Their sexual life
- The commission or alleged commission by them of any offence, or any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

Bishop Challoner only holds personal data which is directly relevant to its employees, customers, contractors and client contacts. That data will be held and processed in accordance with the data protection principles and with this Policy. The following data may be collected, held and processed by the school:

- Identification information relating to employees including, but not limited to, names and contact details, both personal and organisational
- Equal opportunities monitoring information including age, gender, race, nationality and religion
- Health records including details of sick leave, medical conditions, disabilities and prescribed medication
- Employment records including, but not limited to, interview notes, CVs, references from previous employers, application forms, assessments including psychometric assessments, performance reviews and similar documents
- Details of salaries including increases, bonuses, commission, overtime, benefits and expenses, whether within the school or in previous employments, as appropriate
- Records of disciplinary matters including reports and warnings, both formal and informal
- Details of grievances including documentary evidence, notes from interviews, procedures followed and outcomes.

### **General Statement**

The school is committed to maintaining the above principles at all times. Therefore the school will:

- Inform individuals why the information is being collected when it is collected
- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests (see Appendix 1).
- Wherever possible ensure our staff are aware of and understand our policies and procedures
- All staff receive Data Protection training

## **Health Records**

The school holds health records on all employees, which are used to assess the health, wellbeing and welfare of employees and highlight any issues which may require further investigation. Such health records will include details of sick leave, medical conditions, disabilities and prescribed medication. Data under this heading will be used by management only and will not be revealed to fellow employees (unless those employees are responsible for health records in the normal course of their duties).

Employees have the right to request that the school does not keep health records on them. All such requests must be made in writing and addressed to the Compliance Office (Data).

## **Benefits**

In cases where employees are enrolled in benefit schemes which are provided by the school (including, but not limited to, pensions) it may be necessary from time to time for third party organisations to collect personal data from relevant employees.

The school shall not use any such data except insofar as is necessary in the administration of relevant benefits schemes.

## **Monitoring**

Bishop Challoner may from time to time monitor the activities of employees for specific, legal or organisational purposes. Such monitoring may include, but will not necessarily be limited to, internet and email monitoring. The school shall use reasonable endeavours to ensure that there is no intrusion upon employees' personal communications or activities.

Any employee that is to be monitored shall be informed in advance of such monitoring. Monitoring shall not interfere with an employee's normal duties.

## **Processing Personal Data**

Personal data (including sensitive personal data, where appropriate) may be processed by the school in order to:

- Support teaching and learning;
  - Monitor and report on students' progress;
  - Analyse and publish examination results and university destinations of leavers;
  - Provide appropriate pastoral care including medical and other sensitive services;
  - Assess overall performance of the school;
  - Communicate;
  - Collect information for central or national statutory authorities or exam boards;
  - Promote the school and its activities (e.g. events, performances, open days, reunions);
  - Assess and admit students;
  - Recruit and look after students and staff;
  - Monitor email communications or internet access to ensure compliance with school rules and the school's Codes of Conduct; and
  - For other reasonable purposes relating to its operation as a school and employer.
- Further legitimate interests for holding personal data are set out in the school's Privacy Notice

CCTV is used for:

- The prevention, investigation and detection of crime.
- The apprehension and prosecution of offenders (including use of images as evidence in criminal proceedings).
- Safeguarding public, pupil and staff safety.
- Monitoring the security of the site.

### **Data Protection Procedures**

Bishop Challoner shall ensure that all of its employees, contractors, agents, consultants, partners or other parties working on behalf of the school comply with the following when processing and / or transmitting personal data:

- Personal data may be transmitted over secure networks only
- Emails containing personal data shall be stored securely
- Where personal data is to be sent by facsimile transmission the recipient shall be informed in advance of the transmission
- Where personal data is to be transferred in hard copy form it shall be passed directly to the recipient
- All hard copies of personal data shall be stored securely in a locked box, drawer, cabinet or similar
- All electronic copies of personal data shall be stored securely and be password protected.

### **Access by Data Subjects (see appendix)**

A data subject may make a subject access request (“SAR”) at any time to see the information which the school holds about them.

Upon receipt of a SAR the school shall have a maximum period of 30 days within which to respond. The following information will be provided to the data subject:

- Whether or not the school holds any personal data about the person
- A description of any personal data held about the person
- Details of what that personal data is used for
- Details of any third-party organisations that personal data is passed to
- Details of any technical terminology used.

### **Exceptions**

Certain data is exempted from the provisions of the Data Protection Act which includes the following:

- The prevention or detection of crime;
- The assessment of any tax or duty; and
- Where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the School.

The above are examples only of some of the exemptions under the Act

### **Third Parties**

The school will not share data with other organisations or individuals for commercial purposes, unless specific consent is given. We may be required to share some data, including sensitive personal data, with third parties including local authorities, other public authorities, independent school bodies such as the Independent Schools Inspectorate (ISI), health professionals, professional advisors, examination boards or contractors.

The school may also (unless you request otherwise) share personal data about current pupils with the Parents' Association.

### **Notification to the Information Commissioner's Office**

As a data controller, the school is required to notify the Information Commissioner's Office that it is processing personal data. The school is registered in the register of data controllers.

Data controllers must renew their notification with the Information Commissioner's Office on an annual basis. Failure to notify constitutes a criminal offence.

Any changes to the register must be notified to the Information Commissioner's Office within 28 days of taking place.

The Compliance Office (Data) shall be responsible for notifying and updating the Information Commissioner's Office.

### **Review**

The school reserves the right to change this policy at any time.

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the Governing Body and Headteacher.

### **Contacts**

If you have any enquires in relation to this policy, please contact the Headteacher.

## Appendix 1

### Bishop Challoner School

Procedures for responding to subject access requests made under the Data Protection Act 2018 / General Data Protection Regulations (GDPR) 2018.

#### Rights of access to information

Under the Data Protection Act 2018 any individual has the right to make a request to access the personal information held about them by the school.

#### Actioning a subject access request

1. Requests for information should be made in writing; which includes email to data@bcswb.co.uk. If the initial request does not clearly identify the information required, then further enquiries will be made.
2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:
  - passport
  - driving licence
  - utility bills with the current address
  - Birth / Marriage certificate
  - P45/P60
  - Credit Card or Mortgage statement

*This list is not exhaustive.*
3. Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The child's signed written consent will normally be required if they are 12 years or over before the school will disclose any information to the parent(s). The Headteacher may discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.
4. The response time for subject access requests, once officially received, is 30 days (**not working or school days but calendar days, irrespective of school holiday periods**).
5. The Data Protection Act 2018 / General Data Protection Regulations (GDPR) 2018 allows exemptions as to the provision of some information; **therefore all information will be reviewed prior to disclosure.**
6. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the 30 day statutory timescale.

7. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.
8. If there are concerns over the disclosure of information then additional advice should be sought.
9. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.
10. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped. Relevant information from multiple sources may be collated into one document.
11. Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover.
12. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

### **Complaints**

Complaints about the above procedures should be made to the Chairperson of the Governing Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaint procedure.

### **Contacts**

If you have any queries or concerns regarding these policies / procedures then please contact the Headteacher.

Reviewed by: David Rolls

Review Date: August 2023

Date of Next Review: August 2025