


# DATA PROTECTION POLICY

<p><b>Bishop Challoner Catholic College</b></p> 	<b>Next Review</b>	January 2023
	<b>Review Period</b>	Annual
	<b>Principal Reviewed</b>	January 2022
	<b>Website Published</b>	January 2022
	<b>Current Status</b>	Complete
	<b>Staff Owner</b>	J Bloxidge
	<b>Government/DfE Requirement</b>	<b>Statutory</b>
<b>Data Protection Policy</b>		

---

# DATA PROTECTION POLICY

## 1. Introduction

- 1.1 The Data Protection Act 2018 (DPA) replaces the EU Data Protection Directives and the UK's Data Protection Act 1998. Following the UK leaving the EU the DPA is the UK's implementation and of the EU General Data Protection Regulation. In this document, the principles of the EU General Data Protection Regulation as implemented by the DPA are referred to as "GDPR". The purpose of the GDPR is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge and, wherever possible, that it is processed with their consent.
- 1.2 Unless specifically indicated otherwise in this policy, definitions used by the school in this policy are in accordance with definitions contained in the DPA.

## 2. Policy statement

- 2.1 The Board of Governors ("Governors") and management of Bishop Challoner Catholic College ("SMT"), located at Bishop Challoner Catholic College, Institute Road, Kings Heath, B14 7EG are committed to compliance with GDPR in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information Bishop Challoner Catholic College collects and processes in accordance with the GDPR.
- 2.2 Compliance with the GDPR is described by this policy and other relevant policies along with connected processes and procedures.
- 2.3 The GDPR and this policy apply to all of Bishop Challoner Catholic College's personal data processing functions, including those performed on pupils', clients', employees', volunteers', suppliers' and partners' personal data, and any other personal data the organisation processes from any source.
- 2.4 Bishop Challoner Catholic College has established objectives for data protection and Privacy in compliance with GDPR
- 2.5 The Data Protection Officer (DPO) is responsible for reviewing the register of processing annually in the light of any changes to Bishop Challoner Catholic College's activities. This register needs to be available on the supervisory authority's request.
- 2.6 This policy applies to all governors, employees and staff of Bishop Challoner Catholic College and any other interested parties, such as outsourced suppliers of services. Any breach of the GDPR will be referred to the DPO and if applicable dealt with under the disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.
- 2.7 Partners and any third parties working with or for Bishop Challoner Catholic College, and who have or may have access to personal data, will be expected to comply with GDPR. No third party may access personal data held by Bishop Challoner Catholic College without complying with GDPR obligations no less onerous than those to which Bishop Challoner Catholic College is committed.

---

# DATA PROTECTION POLICY

## 3. Responsibilities and roles under the General Data Protection Regulation

- 3.1 Bishop Challoner Catholic College is a data controller and data processor under the GDPR.
- 3.2 The Governors, SMT and all those in managerial or supervisory roles throughout Bishop Challoner Catholic College are responsible for developing and encouraging good information handling practices; responsibilities are set out in individual job descriptions.
- 3.3 The DPO, a role specified in the GDPR, is accountable to the Governors and SMT for the management of personal data within Bishop Challoner Catholic College and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:
  - 3.3.1 development and implementation of the GDPR as required by this policy; and
  - 3.3.2 security and risk management in relation to compliance with the policy.
- 3.4 The DPO, who the Governors and SMT consider to be suitably qualified and experienced, has been appointed to take responsibility for Bishop Challoner Catholic College's compliance with this policy and, in particular, has direct responsibility for ensuring that Bishop Challoner Catholic College complies with the GDPR, as do all managers and supervisors in respect of data processing that takes place within their area of responsibility.
- 3.5 The DPO has specific responsibilities in respect of procedures such as the Subject Access Request Procedure and is the first point of call for employees seeking clarification on any aspect of data protection compliance.
- 3.6 Compliance with data protection legislation is the responsibility of all governors, employees and volunteers of Bishop Challoner Catholic College who process personal data.
- 3.7 All staff are required to have undertaken data protection awareness training, the nature of which will be decided by the frequency of processing and the nature of the personal data they may process.

## 4. Data protection principles

All processing of personal data must be conducted in accordance with the data protection principles as set out in the EU General Data Protection Regulation and the DPA. Bishop Challoner Catholic College's policies and procedures are designed to ensure compliance with the principles.

### 4.1 Personal data must be processed lawfully, fairly and transparently

Lawful – identify a lawful basis before you can process personal data. These are often referred to as the “conditions for processing”, for example consent.

Fairly – in order for processing to be fair, the data controller has to make certain information available to the data subjects. This applies whether the personal data was obtained directly from the data subjects or from other sources. The GDPR has increased requirements about what information should be available to data subjects, which is covered in the ‘Transparency’ requirement.

Transparently – the GDPR includes rules on giving privacy information to data subjects. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language.

---

# DATA PROTECTION POLICY

Bishop Challoner Catholic College's Privacy Notice Procedure is set out in the school's policies.

- 4.2 Personal data can only be collected for specific, explicit and legitimate purposes Data obtained for specified purposes must not be used for a purpose that differs from those set out as part of Bishop Challoner Catholic College's GDPR register of processing.
- 4.3 Personal data must be adequate, relevant and limited to what is necessary for processing
  - 4.3.1 The Data Protection Officer is responsible for ensuring that Bishop Challoner Catholic College does not collect information that is not necessary for the purpose for which it is obtained.
  - 4.3.2 All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must be in accordance with the school's privacy policies and if appropriate, approved by the DPO.
  - 4.3.3 The DPO will ensure that data collection methods are reviewed periodically to ensure that collected data continues to be adequate, relevant and not excessive.
- 4.4 Personal data must be accurate and kept up to date with every effort to erase or rectify without delay
  - 4.4.1 Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.
  - 4.4.2 The DPO is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.
  - 4.4.3 It is also the responsibility of the data subject to ensure that data held by Bishop Challoner Catholic College is accurate and up-to-date. Completion of a registration or application form by a data subject will include a statement that the data contained therein is accurate at the date of submission.
  - 4.4.4 Governors, employees, staff and pupils should be required to notify Bishop Challoner Catholic College of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of Bishop Challoner Catholic College to ensure that any notification regarding change of circumstances is recorded and acted upon.
  - 4.4.5 The DPO is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.
  - 4.4.6 On at least an annual basis, the DPO will review the retention dates of all the personal data processed by Bishop Challoner Catholic College, and will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted or destroyed in accordance with school policies.
  - 4.4.7 The DPO is responsible for responding to requests for rectification from data subjects within the prescribed timescales. If Bishop Challoner Catholic College decides not to comply with the request, the DPO or SMT must respond to the data subject to explain its reasoning and inform them of their right to complain to the ICO and seek judicial remedy.

---

# DATA PROTECTION POLICY

- 4.5 Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.
- 4.5.1 Where personal data is retained beyond the processing date, it will be minimized, encrypted or pseudonymised in order to protect the identity of the data subject in the event of a data breach.
  - 4.5.2 Personal data will be retained in line with the current Records Retention Schedule, Information and Records Management Society's (IRMS) Information Management Toolkit for Schools and, once its retention date is passed, it must be securely deleted or destroyed.
  - 4.5.3 The DPO must specifically approve any data retention that exceeds the defined retention periods and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.
- 4.6 Personal data must be processed in a manner that ensures the appropriate security The DPO is responsible for the manner of processing of data by governors employees and staff in the school taking into account all the circumstances of Bishop Challoner Catholic College's controlling or processing operations.

In determining appropriateness, the DPO should also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or pupils) if a security breach occurs, the effect of any security breach on Bishop Challoner Catholic College itself, and any likely reputational damage including the possible loss of trust.

When assessing appropriate technical measures, the DPO will consider the following:

- Password protection;
- Automatic locking of idle terminals;
- Removal of access rights for USB and other memory media;
- Virus checking software and firewalls;
- Role-based access rights including those assigned to temporary staff;
- Encryption of devices that leave the organisations premises such as laptops;
- Security of local and wide area networks;
- Privacy enhancing technologies such as pseudonymisation and anonymisation;
- Identifying appropriate and relevant national or international security standards.

When assessing appropriate organisational measures the DPO will consider the following:

- The appropriate training levels throughout Bishop Challoner Catholic College;
- Measures that consider the reliability of employees (such as references, etc.);
- The inclusion of data protection in employment contracts;
- Identification of disciplinary action measures for data breaches;
- Monitoring of staff for compliance with relevant security standards;
- Physical access controls to electronic and paper based records;
- Adoption of a clear desk policy;
- Storing of paper based data in lockable fire-proof cabinets;
- Restricting the use of portable electronic devices outside of the workplace;
- Restricting the use of employee's own personal devices being used in the workplace;
- Adopting clear rules about passwords;
- Making regular backups of personal data and storing the media off-site;
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the EEA.

---

# DATA PROTECTION POLICY

These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

## 4.7 The controller must be able to demonstrate compliance with the GDPR's other principles (accountability)

The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements.

Bishop Challoner Catholic College will demonstrate compliance with the data protection principles by (as applicable); implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design and by default, data protection impact assessments (DPIAs), breach notification procedures and incident response plans.

## 5. Data subjects' rights

### 5.1 Data subjects have the following rights regarding data processing, and the data that is recorded about them:

- 5.1.1 To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- 5.1.2 To prevent processing likely to cause damage or distress.
- 5.1.3 To prevent processing for purposes of direct marketing.
- 5.1.4 To be informed about the mechanics of automated decision-taking process that will significantly affect them.
- 5.1.5 To not have significant decisions that will affect them taken solely by automated process.
- 5.1.6 To sue for compensation if they suffer damage by any contravention of the GDPR.
- 5.1.7 To take action to rectify, block, erase, including the right to be forgotten, or destroy inaccurate data.
- 5.1.8 To request the ICO to assess whether any provision of the GDPR has been contravened.
- 5.1.9 To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.
- 5.1.10 To object to any automated profiling that is occurring without consent.

### 5.2 Bishop Challoner Catholic College ensures that data subjects may exercise these rights:

- 5.2.1 Data subjects may make data access requests
- 5.2.2 Data subjects have the right to complain to Bishop Challoner Catholic College related to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled in line with Bishop Challoner Catholic College's standard Complaints Procedure.

## 6. Consent

### 6.1 Bishop Challoner Catholic College understands 'consent' to mean that it has been freely

---

# DATA PROTECTION POLICY

given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement, by omission or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.

- 6.2 Bishop Challoner Catholic College understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them as consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.
- 6.3 In most cases, there must be some active communication between the parties to demonstrate active consent.
- 6.4 The controller must be able to demonstrate that consent was obtained for the processing operation.
- 6.5 For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.
- 6.6 In most instances, consent to process personal and sensitive data is obtained routinely by Bishop Challoner Catholic College using standard consent documents or statements on forms.
- 6.7 Where Bishop Challoner Catholic College provides online services to children, parental or custodial authorisation must be obtained as required

## 7. Security of data

- 7.1 All governors, employees and volunteers are responsible for ensuring that any personal data that Bishop Challoner Catholic College holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by Bishop Challoner Catholic College to receive that information and has entered into a confidentiality agreement.
- 7.2 All personal data should be accessible only to those who need to use it, and access may only be granted in line with the access control policy. All personal data should be treated with the highest security and must be kept:
  - in a lockable room with controlled access; and/or
  - in a locked drawer or filing cabinet; and/or
  - if computerised, password protected in line with corporate requirements in the Access Control Policy; and/or
  - Stored on computer media which are encrypted in line with Secure Disposal of Storage Media.
- 7.3 Care must be taken to ensure that PC screens and terminals are not visible except to authorised personnel. All governors, employees and volunteers are required to enter into an Acceptable Use Agreement before they are given access to organisational information of any sort.
- 7.4 Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit authorisation. As soon as manual records are no longer required for day-to-day business use, they must be removed to secure archiving or securely destroyed.
- 7.5 Personal data may only be deleted or disposed of in line with the Records Retention Procedure, Information and Records Management Society's (IRMS) Information Management Toolkit for Schools. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed before disposal.
- 7.6 Processing of personal data 'off-site' presents a potentially greater risk of loss, theft

---

# DATA PROTECTION POLICY

or damage to personal data. Staff must be especially diligent when authorised to process data off- site.

## 8. Disclosure of data

- 8.1 Bishop Challoner Catholic College must ensure that personal data is not disclosed to unauthorised third parties which may include family members, friends, government bodies, and in certain circumstances, the Police. All governors and employees should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of Bishop Challoner Catholic College's business.
- 8.2 The GDPR permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:
- to safeguard national security;
  - prevention or detection of crime including the apprehension or prosecution of offenders;
  - assessment or collection of tax duty;
  - discharge of regulatory functions (includes health, safety and welfare of persons at work);
  - to prevent serious harm to a third party; and
  - to protect the vital interests of the individual in life and death situations.
- 8.3 All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the DPO.

## 9. Retention and disposal of data

- 9.1 Bishop Challoner Catholic College shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.
- 9.2 Bishop Challoner Catholic College may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.
- 9.3 The retention period for each category of personal data will be set out in the Records Retention Procedure, Information and Records Management Society's (IRMS) Information Management Toolkit for Schools along with the criteria used to determine this period including any statutory obligations Bishop Challoner Catholic College has to retain the data.
- 9.4 Personal data must be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subjects. Any disposal of data will be done in accordance with the secure disposal procedure.



---

# DATA PROTECTION POLICY

## 10. Data transfers

10.1 All exports of data from within the UK or European Economic Area ("EEA") countries to non-EEA countries (referred to in the GDPR as 'third countries') are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects".

The broader area of the EEA is granted 'adequacy' on the basis that all such countries are signatories to the GDPR. The non-EU EEA member countries (currently Liechtenstein, Norway and Iceland) apply EU regulations through a Joint Committee Decision.

The transfer of personal data outside of the EEA is prohibited unless one or more of the specified safeguards, or exceptions, apply:

### 10.1.1 An adequacy decision

The government can and does assess third countries, a territory and/or specific sectors within third countries to assess whether there is an appropriate level of protection for the rights and freedoms of natural persons. In these instances no authorisation is required.

Countries that are in the EU and members of the European Economic Area (EEA) but not of the EU are accepted as having met the conditions for an adequacy decision.

### 10.1.2 Privacy Shield

If Bishop Challoner Catholic College wishes to transfer personal data from the EU to an organisation in the United States it should check that the organisation is signed up with the Privacy Shield framework at the US Department of Commerce (DOC). The obligation applying to companies under the Privacy Shield are contained in the "Privacy Principles". The US DOC is responsible for managing and administering the Privacy Shield and ensuring that companies live up to their commitments. In order to be able to certify, companies must have a privacy policy in line with the Privacy Principles e.g. use, store and further transfer the personal data according to a strong set of data protection rules and safeguards. The protection given to the personal data applies regardless of whether the personal data is related to an EU resident or not. Organisations must renew their "membership" to the Privacy Shield on an annual basis. If they do not, they can no longer receive and use personal data from the EU under that framework.

#### Assessment of adequacy by the data controller

In making an assessment of adequacy, the UK based exporting data controller should take account of the following factors:

- the nature of the information being transferred;
- the country or territory of origin and final destination of the information;
- how the information will be used and for how long;
- the laws and practices of the country of the transferee, including relevant codes of practice and international obligations; and
- the security measures that are to be taken as regards the data in the overseas location.

---

# DATA PROTECTION POLICY

## 10.1.3 Binding corporate rules

Bishop Challoner Catholic College may adopt approved binding corporate rules for the transfer of data outside the EU. This requires submission to the relevant supervisory authority for approval of the rules that Bishop Challoner Catholic College is seeking to rely upon.

## 10.1.4 Model contract clauses

Bishop Challoner Catholic College may adopt approved model contract clauses for the transfer of data outside of the EEA. If Bishop Challoner Catholic College adopts model contract clauses approved by the ICO there is an automatic recognition of adequacy.

## 10.1.5 Exceptions

In the absence of an adequacy decision, Privacy Shield membership, binding corporate rules and/or model contract clauses, a transfer of personal data to a third country or international organisation shall only take place on one of the following conditions:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; and/or
- The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

## 11. Information asset register/data inventory

11.1 Bishop Challoner Catholic College has established a Personal Data Inventory and identifies data flows as part of its approach to addressing risks, thus determining:

- business processes that use personal data;
- sources of personal data;
- volume of data subjects;
- description of each item of personal data;
- processing activity;
- who maintains the inventory of data categories of personal data processed;
- who documents the purpose(s) each category of personal data is used for;
- recipients and potential recipients of the personal data;
- the role of the Bishop Challoner Catholic College throughout the data flow;
- key systems and repositories;
- any data transfers, including overseas; and
- All retention and disposal requirements.

---

# DATA PROTECTION POLICY

- 11.2 Bishop Challoner Catholic College is aware of any risks associated with the processing of particular types of personal data.
  - 11.2.1 Bishop Challoner Catholic College assesses the level of risk to individuals associated with the processing of their personal data. Data protection impact assessments (DPIAs) are carried out in relation to the new collection and processing of personal data by Bishop Challoner Catholic College, and in relation to processing undertaken by other organisations on behalf of Bishop Challoner Catholic College.
  - 11.2.2 Bishop Challoner Catholic College shall manage any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.
  - 11.2.3 Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, Bishop Challoner Catholic College shall, prior to the processing, carry out a DPIA of the impact of the envisaged processing operations on the protection of personal data. A single DPIA may address a set of similar processing operations that present similar high risks.
  - 11.2.4 Where, as a result of a DPIA it is clear that Bishop Challoner Catholic College is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether or not Bishop Challoner Catholic College may proceed must be escalated for review to the DPO.
  - 11.2.5 The DPO shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the ICO.
  - 11.2.6 Appropriate controls will be applied to reduce the level of risk associated with processing individual data to an acceptable level and the requirements of the GDPR.

## Document Owner and Approval

The DPO is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above. A current version of this document is available to all members of staff via the school website and the staff teams area.