

Classification:

Public

Data Protection



**Bishop
Perowne**
Church of England College
Endeavour Forever

Title: Data Protection

Document Type: Policy and Procedure

Document Reference: GEN-01

Version: 2.0

Status: Approved

Review: Full Governing Board

Reviewed: 19th August 2022

Next Review Date: 18th August 2024

Document Management

A. Identification

Business Unit	Description
Document Type	Policy and Procedure
Document Name:	Data Protection
Document Code:	GEN-04
Document Category:	General
Review Cycle:	2 Years
File Name	GEN-04 Data Protection Procedures v2.0.docx
Classification	Public (everyone can see the information)

B. Document contributors

Name	Position	Author	Reviewer	Approver
Peter Albertini	Business Manager	✓		
Karen Wigley	Headteacher's P.A.		✓	
Mrs A Iddon	Chair of Governors			✓
Jane Price	Headteacher			✓

C. Approval

This document is a controlled document authorized for release once all signatures have been obtained or has been approved for release at either a Full Governing Board meeting or relevant sub-committee meeting. Approval of this document constitutes approval of the content as described herein.

Name	Position	Date	Signature
Anita Iddon	Chair of Governors	August 2022	<i>A Iddon</i>
Jane Price	Headteacher	August 2022	<i>J Price</i>

D. Document revision

Date	Revision	Modification	Modified by
24/01/2017	0.1	Creation of initial version for review using new document template and inclusion of new sections on awareness and glossary	Iain Williams
16/09/2020	1.0	Policy reviewed	Ryan Ramsden
19/08/2022	2.0	Policy reviewed	Karen Wigley

Table of contents

1	OVERVIEW.....	4
1.1	Purpose	4
1.2	Scope.....	4
1.3	Related documents	4
1.4	Reviews	4
1.5	Equality Impact Assessment	4
2	RESPONSIBILITY FOR THE POLICY AND PROCEDURE.....	5
2.1	Role of the Governing Body	5
2.2	Role of the Headteacher.....	5
3	POLICY AND PROCEDURES	6
3.1	Introduction.....	6
3.2	Compliance with the Data Protection Act 2018	6
3.3	The Data Controller.....	7
3.4	Information Asset Owners.....	7
3.5	Responsibilities of staff	7
3.6	Responsibilities of parents/carers.....	7
3.7	Data Security	8
3.8	Retention of Data.....	8
3.9	Disposal of Data.....	9
3.10	Rights to Access Information	9
3.11	Compliance.....	9
3.12	Registration with the Information Commissioner’s Office (ICO)	10
3.13	Loss or mismanagement.....	10
3.14	Training and awareness.....	10
4	RAISING AWARENESS OF THIS POLICY	11
4.1	Promoting Awareness	11
4.2	Training	11
4.3	Monitoring the Effectiveness of the Policy	11
5	GLOSSARY.....	12

1 OVERVIEW

1.1 Purpose

Refer to Section 3 Policies and Procedures

1.2 Scope

Refer to Section 3 Policies and Procedures

1.3 Related documents

Refer to Section 3 Policies and Procedures

1.4 Reviews

Refer to Section 3 Policies and Procedures

1.5 Equality Impact Assessment

Under the Equality Act 2010 the College is obliged not to discriminate against people on the basis of age, disability, gender, gender identity, pregnancy or maternity, race, religion or belief and sexual orientation.

This policy has been equality impact assessed and the Governing Body believes that it is in line with the Equality Act 2010 as it is fair, it does not prioritise or disadvantage any pupil or any other connected party and it helps to promote equality at the College.

2 RESPONSIBILITY FOR THE POLICY AND PROCEDURE

2.1 Role of the Governing Body

The Governing Body has:

- delegated powers and responsibilities to the Headteacher to ensure all school personnel and visitors to the school are aware of and comply with this policy;
- responsibility for ensuring this policy and all policies are maintained and updated regularly;
- responsibility for ensuring all policies are made available to parents;
- nominated a link governor to visit the school regularly, to liaise with the Headteacher and the coordinator and to report back to the Governing Body;
- responsibility for the effective implementation, monitoring and evaluation of this policy

2.2 Role of the Headteacher

The Headteacher will:

- ensure all school personnel, students and parents are aware of and comply with this policy;
- work closely with the link governor and coordinator;
- provide guidance, support and training to all staff;
- monitor the effectiveness of this policy;

3 POLICY AND PROCEDURES

3.1 Introduction

Bishop Perowne C of E College holds and processes information about its students, parents/carers, applicants, staff and other individuals who come into contact with the College and who are defined as “data subjects” by the Data Protection Act 2018.

The College produces, processes and stores various types of personal data including information on attendance, academic progress, health and safety factors and other data that the College is required to hold by law.

In addition, the College may be legally required to collect and use certain types of information to comply with statutory obligations of local authorities, government entities and other bodies.

3.2 Compliance with the Data Protection Act 2018

The College takes the protection of all personal data very seriously. To comply with the law, the College must collect and use personal information fairly, store it safely and not disclose it to any other person unlawfully. Personal information must be dealt with properly regardless of how it is collected, recorded and used, whether on paper or in electronic form.

To this end the College fully endorses and seeks to adhere to the principles of data protection, as set out in the Data Protection Act 1998. Specifically, these principles require that personal information:

- Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met;
- Shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;
- Shall be adequate, relevant and not excessive in relation to the purpose for which the data is originally processed;
- Shall be accurate and, where necessary, kept up to date;
- Shall not be kept for longer than is necessary;
- Shall be processed in accordance with the rights of data subjects under the Act;
- Shall be safeguarded and appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data;
- Shall not be transferred to a country or territory outside 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.

The College and all staff who process, hold or use any personal information must ensure that they follow these principles at all times.

3.3 The Data Controller

The Governing Body is responsible for the implementation of the terms of the Data Protection Act and is responsible for appointing a Data Controller who has specific responsibilities for data protection within the College. This includes annual registration with the Information Commissioner's Office as required by the Data Protection Act (see section 12 below).

The Data Controller will be familiar with information risks and the organisation's response, take ownership of the College's Data Protection Policy, and act as an advocate for information risk management.

The Data Controller is the Headteacher.

The Data Protection Officer is the Headteacher's P.A.

3.4 Information Asset Owners

The College has also identified Information Asset Owners (IAOs) for the various types of data being held in College (such as student and staff information, and assessment data).

These IAOs will manage and address risks to the information and understand what information is held and for what purpose, how information has been amended or added to over time, and who has access to protected data and why. They will ensure that information in their care is protected by an appropriate level of security via, for example, password protection or where necessary, encryption.

The IAOs are:

- SIMS/data: the data manager
- Exams: the examinations officer
- Staff: the Headteacher's PA
- ICT Support: the IT technician
- Safeguarding: the College Designated Safeguarding Lead
- SEN: the SENCO
- Student archives: the Headteacher's PA

3.5 Responsibilities of staff

All staff are responsible for:

- Checking that any information they provide to the College in connection with their employment is accurate and up to date;
- Informing the College of any changes to information which they have provided, e.g. changes of name, address, home email address and telephone numbers; and
- Informing the College of any errors in the information that the College holds about them.

3.6 Responsibilities of parents/carers

All parents/carers are responsible for:

- Checking that any information they provide to the College is accurate and up to date;
- Informing the College of any changes to information which they have provided, e.g. changes of address, telephone numbers; and
- Informing the College of any errors in the information that the College holds about them if they become aware of such errors.

The College cannot be held responsible for any errors in the above information of which it has not been informed.

3.7 Data Security

All staff are responsible for ensuring that any personal information which they hold, or for which they are responsible, is kept securely.

This could include information about a variety of members of the College community (including students, staff and parents/carers), and cover a wide range of subject-matter, such as reports, results, disciplinary records, guardianship issues, references, employment history, tax information, national insurance records and staff appraisal records.

Members of staff must take particular care when handling sensitive personal data – for students this would not only include addresses, phone numbers and dates of birth but could also include information about medical issues, special educational needs, domestic background, child protection concerns, personal beliefs and opinions, and psychological and emotional factors.

The following data security rules are to be observed by members of staff at all times:

- Personal information stored in electronic form must be password protected;
- Computers used to access personal information must be locked whenever they are left unattended;
- Personal information must be kept on the network storage facilities provided;
- Personal information that is collected or processed over the Internet must only be accessed via a secure encrypted connection using username authentication to prevent unauthorised disclosure;
- Personal information must not be transferred via email;
- Personal information must not be disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party; and
- All staff must abide by the policies and procedures laid out in the Staff Handbook that have a bearing on data protection matters.

3.8 Retention of Data

The College will keep different types of information for differing lengths of time, depending on legal, academic and operational requirements.

Advice on the collection, retention and secure storage of information may be obtained from the Data Controller.

3.9 Disposal of Data

The College will comply with the requirements for the safe destruction of personal data when it is no longer required. The disposal of 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 for data.

When it is time to destroy stale-dated paper files archived in boxes that contain sensitive information, these must first be cleared for destruction by the Headteacher's PA before they are released for on-site shredding every August.

This purpose of this check is to ensure that only the correct files are destroyed and to minimise the risk of accidental destruction of records that are still current.

Members of staff who have small volumes of confidential papers that should be destroyed (for example, draft student reports, draft financial statements) may use the shredders in the staff room or outside the reprographics room and do not need to consult the Headteacher's PA before disposing of such material.

3.10 Rights to Access Information

All data subjects have the right to access any personal information that is still held about them. They also have the right to have inaccurate data corrected, destroyed or erased.

Any person who wishes to exercise this right should contact the College's Data Controller in writing. The letter should include the requestor's name and contact details. The College may ask for further information in order to confirm the requestor's identity.

The College reserves the right to make a charge of up to £10 for each access request. The College will comply with the request within one month from the date that the written request is received.

3.11 Compliance

Unauthorised disclosure of personal information is a breach of the Data Protection Act 1998 and may result in disciplinary action. In some cases it may be considered as gross misconduct and may result in a personal liability for the individual staff member.

Any data subject who feels that this Data Protection Policy has not been correctly followed with regard to personal information about themselves, should raise the matter initially with the Data Controller. If they feel that the matter has not been resolved it should be raised as a formal grievance.

3.12 Registration with the Information Commissioner's Office (ICO)

The College is registered with the ICO, which is the UK's independent body set up to uphold information rights and oversee compliance with data protection legislation.

The College automatically renews its registration on an annual basis each July by paying the required fee by direct debit. The School Business Manager is responsible for ensuring that the College's registration with the ICO remains current and that annual fees are paid.

3.13 Loss or mismanagement

It is imperative that any loss or mismanagement of information is reported as soon as it is recognized. In the event of a security lapse, staff should:

- Immediately inform the Data Controller, recording the time and date when the loss was identified and the nature of the data lost; and
- Record any details regarding the loss of data, for example, where the loss occurred and any staff or students present at the time.

The Data Controller will provide the Information Commissioner's Office (ICO) with details regarding the time and place of loss, or when loss was identified, and of the nature of the data and potential risk.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a governor.

3.14 Training and awareness

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; and
- Staff meetings/briefings.

4 RAISING AWARENESS OF THIS POLICY

This policy is a public document and will be made available to any interested stakeholder.

4.1 Promoting Awareness

We will raise awareness of this policy via:

- The school website www.bishopperowne.co.uk
- Meetings with school personnel and volunteers
- Reports such as the annual report to parents and Headteacher reports to the Governing Body

4.2 Training

All school personnel:

- Receive training on induction which specifically covers:
 - All aspects of this policy
- Receive periodic training so that they are kept up to date with new information;
- Receive equal opportunities training on induction in order to improve their understanding of the Equality Act 2010 and its implications.

4.3 Monitoring the Effectiveness of the Policy

The practical application of this policy will be reviewed annually or when the need arises.

5 GLOSSARY

Glossary of terms used within this policy and procedure document. For the full Glossary of terms used at Bishop Perowne CE College, please refer to the document "REF-02 Glossary of Terms".

I	
IAO	Information Asset Owners
ICO	Information Commissioner's Office

S	
SEN	Special Educational Needs
SENCO	Special Educational Needs Coordinator

Any enquiries regarding this publication should be sent to us at

Bishop Perowne C. of E. College,
Merriman's Hill Road,
Worcester,
Worcestershire,
WR3 8LE

T: 01905 746800

F :01905 746846

E: info@bishopperowne.co.uk

This document is also available from
our website at
www.bishopperowne.co.uk