Bishopshalt School

Data Protection (GDPR) Policy

Responsibility	Mr P Edgley	Date reviewed	May 2021
Headteacher	Mr McGillicuddy	Next review date	May 2022
Ratified by	Governing Body	Date Ratified	May 2021

Data Protection Policy (GDPR) 2021

1. Introduction

This policy lays out how Bishopshalt School (the School) will comply with its responsibilities under the General Data Protection Regulations (GDPR) 2018 (the Act).

All School employees, contractors and governors will be bound by its conditions and will be responsible for compliance with the policy and the Act.

This policy applies to all information that is subject to the Act. This includes all personal data that is processed automatically, any personal data held in a manual form in a relevant filing system and any personal data held in an accessible record.

The School will nominate a Data Protection Officer to oversee the implementation of this policy and to produce guidelines to achieve the standards laid out in this policy.

A monitoring process will be developed to ensure compliance with this policy.

The School will produce guidelines to support this policy which are accessible to students age 13 years plus.

The School may take disciplinary action over any breach of the Act and/or this policy by an employee.

2. Definitions

Personal Data – Any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

Sensitive Personal Data - Sensitive personal data includes data relating to the following:

· Racial or ethnic origin

· Political opinions

· Religious or philosophical beliefs

· Trade union membership

· Genetic data

· Biometric data

· Health

· Sex life

· Sexual orientation

Data Controller – Legal person or persons who decide the purpose for which personal data are to be processed. In this instance the School is the data controller for all personal date it processes.

Data Processor – A person (other than an employee of the data controller) who processes personal data on behalf of a data controller.

Data Protection Officer – The person responsible for ensuring that personal data is handled and stored appropriately, The School's data protection officer is the Director of Finance and Business.

Data Subject – an individual who is the subject of personal data.

Principles – There are six data protection principles which personal data must be processed in accordance with.

3. Six Principles of the GDPR

GDPR stipulates six data protection principles that must be adhered to when processing personal data to ensure that it is:

I. Processed Fairly, Lawfully and in a Transparent Manner
The school will ensure that the personal data the school is collecting, storing, using, sharing or processing in any way is being done so fairly and lawfully. There will be a legal basis for using the data and data subjects will be informed about:
   a. · What personal data the school is using
   b. · What specific purpose the data is used for
   c. · If it is to be shared, details of who it is to be shared with (name of the company/supplier etc.)
   d. · How long it will be stored for and/or processed
   e. · The identity of the Data Controller
   f. · Name and contact details of the Data Protection Officer
   g. · Their subject rights and how to exercise these

II. Used for Specified, Explicit and Legitimate Purposes.
Once the data subject has been informed of what data the school is using and why, the school cannot use that data for another purpose without first making the data subject aware.

III. Used in a way that is Adequate, Relevant and Limited.
The school will ensure that it uses only as much personal data as is required for the specific purpose and no more.

IV. Accurate and Kept Up-to-Date
The school will endeavour to ensure all personal data is accurate when it is obtained and kept up-to-date.

V. Kept no Longer than is Necessary
The school will only retain personal data for as long as it is required for the processing specified. Once it is no longer needed it will be securely destroyed/erased

unless there is a legitimate reason to keep it – such as legal requirements, the need to retain financial records etc.
The school will follow the guidelines outlined in the Data Retention Policy which suggests that the majority of pupil data should be retained until the pupil reaches 25 years of age, except in special circumstances. In primary schools, guidelines suggest that the data should be retained whilst the pupil is attending the school and then should move with the pupil to their next educational establishment.

VI. Processed in a Manner that Ensures Appropriate Security of the Data
The school will protect personal data against unauthorised or unlawful processing, accidental loss, destruction or damage through appropriate technical and organisational measures.
Technical measures will include firewalls to prevent unauthorised access, encryption of the data in any software the school uses or strong passwords in place that are forced to be frequently changed.

4. Notification

Under the Act, Data Controllers are required to notify the Information Commissioner of the processing which they undertake.

The School will maintain its register entry and regularly review its processing to ensure that its register entry is accurate and up to date.

5. Data Subject Rights

Much of the data held in schools falls under 'Public Interest'* and therefore consent will not be required, and therefore cannot be withdrawn, in relation to that data. A long side the 'Public Interest' criteria data subjects have the following rights:

· The right to be informed – they must be told what data is being used, why and for what purpose

· The right of access – they have to be allowed to see what data of theirs you are processing if they request it

· The right of rectification – if their data is wrong, it must be corrected

· The right to erasure – *they can demand that you erase all data of theirs that you have

· The right to restrict processing – *they can demand that you stop using their data unless you have a legitimate legal basis for continuing to do so

· The right to data portability – *they can decide to move their data to another processor and you have to provide them with all their data so they can do this

· The right to object – *they can object to your use of their data and you must stop using it unless you have an overriding legitimate reason to continue.

· Rights in relation to automated decision making or profiling – they can

demand that automated decisions about them are reviewed by a human

6. Complaints, Enforcement and Dealing with Breaches

All complaints regarding Data Protection are to be passed immediately to the Data Protection Officer.

Any School employees, contractors or governors who suspects that a breach of the Act has or will occur, must report it to the Data Protection Officer.

Under GDPR all data breaches which have the potential to have a significant detrimental effect on the individual(s) through discrimination, damage to reputation, financial loss, loss of confidentiality or any other economic or social disadvantage must be reported by the data controller to the ICO within 72 hours of discovery.

If the breach is potentially a 'high risk' to the individual(s) affected then the school must also notify the data subject(s).

Data breaches occur for a wide variety of reasons, including loss or theft of equipment, unauthorised access to data, unforeseen circumstances such as fires or flooding and the majority are caused by mistakes or carelessness rather than hacking or viruses.

The school will follow its procedures in relation to a data breaches by:

· Responding quickly

· Assessing the risk to data subjects

· Investigating the cause

· Reporting to the ICO (if necessary)

· Implementing measures to prevent recurrence

All School staff, contractors and governors are expected to cooperate in full with any investigation undertaken by the Data Protection Officer, or the Information Commissioner into an alleged breach of the Act.

Contact Information

7. The School's Data Protection Officer can be contacted at:

Mr P Edgley

Director of Resources

Bishopshalt School

Royal Lane

Hillingdon

Uxbridge

UB8 3RF

More information about the Data Protection Act is available from:

The Information Commissioner's Office

Wycliff House

Water Lane

Wilmslow

Cheshire

SK9 5AF

Telephone: 0303 123 1113

www.ico.gov.uk

8. Monitoring and Review

This policy will be reviewed after one year in the first instance and therefore after every two years.

The person responsible for organising the review process is the Director of Finance and Business.

This revision was published on 25 April 2018

Description of Processing

The following is a broad description of the way Bishopshalt School processes personal information. For a data subject to understand how their personal information is process they may need to refer to any personal communication they have received, check any privacy notices the school had provided or contact the school to ask about their personal circumstances.

Nature of the Work: Academy

Reasons/purpose for processing information:

We process personal information to enable us to provide:

· education

· training

· welfare and educational support services

and to:

· administer school property

· maintain our own accounts and records

· undertake fundraising

· support and manage our employees

We also use CCTV for:

· student safety

· security

· the prevention and detection of crime

Types and classes of information processed:

We process information relevant to the above reasons and purposes. This may include:

- Personal details
- Family details
- Education and employment details
- Financial details
- Goods and services
- Disciplinary and attendance records
- Vetting checks
- DBS checks
- Visual images, personal appearance and behaviour
- Lifestyle and social circumstances

We also process sensitive classes of information that may include:

- Physical or mental health details
- Racial or ethnic origin
- Religious or other beliefs
- Trade union membership
- Sexual life
- Information about offences or alleged offences

Who the information is processed about:

We process personal information about:

- Employees
- Students
- Professional experts and advisers
- Members of the governing body
- Sponsors and supporters
- Suppliers and service providers

Complainants

Enquirers

Individuals captured by CCTV images

Who the information may be shared with:

We sometimes need to share the personal information we process with individuals themselves and also other organisations. Where this is necessary we are required to comply with all aspects of the Data Protection Act (GDPR) what follows is a description of the types of organisations we may need to share some of the personal information we process with for one or more reasons.

Where necessary or required we share information with:

· Family, associates and representatives of the person whose personal data we are processing

· Educators and examining bodies

· Careers services

· The Governing Body

· Local and central Government

· Healthcare, social and welfare organisations

· Police forces and courts

· Current, past and prospective employers

· Voluntary and charitable organisations

· Business associates

· Professional advisers

· Suppliers and service providers

· Financial organisations

· Press and media

Transferring information overseas

We do not transfer any personal information outside the European Economic Area (EEA).