St Bernadette's Catholic Primary School

Data Protection Policy (UK GDPR)

"Doing our best for God"

Data Protection Policy

(UK GDPR)

1. Introduction

St Bernadette's Primary School collects, holds and processes personal data about pupils, staff, parents/carers, governors, visitors and other individuals who have contact with the school. It has a number of legal obligations under the UK General Data Protection Regulation (UK GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018).

St Bernadette's Primary School is defined as a data controller, as it 'determines the purpose and means of processing of personal data' and as such it pays an annual fee to Information Commissioner's Office as required by the Data Protection (Charges and Information) Regulations 2018.

This policy commits that the school will also comply with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, the Protection of Freedoms Act 2012 when referring to use of biometric data and Article 8 of the Human Rights Act 1998.

2. Scope

This policy applies to all personal data held as information in any format including paper, electronic, images and sound, and emails that may be sent or received by the school.

All stages of the lifecycle of personal data are covered by this policy:

- Obtaining of data;
- Storage and security of data and any information this data creates;
- Use and disclosure of data and any information this data creates;
- Sharing of data and any information this data creates;
- Disposal and destruction of data and any information this data creates.

This policy applies to all part-time and full-time employees, including those working from home and from other locations and all other workers (including casual and agency workers, secondment posts and contractors) using the school's equipment and computer network. This policy also applies to volunteers and students (including work experience or work-placement).

3. Definitions

The UK GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The UK GDPR refers to sensitive personal data as 'special categories of personal data'. Special category data is personal data which the UK GDPR says is more sensitive, and so needs more protection. For example, information about an individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics, health, sex life or sexual orientation, are all 'special categories of personal data'.

4. Data Protection Principles

Article 5 of the UK GDPR sets out seven key principles which lie at the heart of the general data protection regime.

Article 5(1) requires that personal data shall be:

a. Processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency').

b. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes […] ('purpose limitation').

c. Adequate, relevant and limited to what is necessary in relation to the purpose for which they are process ('data minimisation').

d. Accurate and, where necessary, kept up to date; every reasonable step to ensure inaccurate data are erased or rectified without undue delay ('accuracy').

e. Kept in a form which permits identification of the individual for no longer than is necessary for the purpose which the data are processed […] ('storage limitations').

f. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

5. Lawful Processing

The school will only process personal data if one of the following conditions are met, which are outlined in Article (6)(1) of the UK GDPR:

- Data subject has given consent to the processing of their personal data. This consent will be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data

subject's wishes. Consent will be recorded and once withdrawn by the data subject, the school will cease processing data for the specified purpose without undue delay.
- Processing is necessary for the performance of a contract to which the data subject are a party to, or in order to take steps at the request of the data subject prior to entering the contract.
- Processing is necessary for compliance with a legal obligation to which the school is subject to.
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the school or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

The school will only collect and process 'special categories of personal data' if one of the additional conditions set out in Article 9(2) has been satisfied.

6. Consent

In all cases, consent must be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's wishes. The school is therefore committed to obtaining consent in the following manner:

- Consent is presented in a manner clearly distinguishable from other matters.
- The request is made in an intelligible and easily accessible form using plain language.
- Is freely given (i.e. not based on the need to conduct another processing activity).
- The date, method, validity and content of the consent is documented.
- A simple method is provided for the data subject to be able to withdraw consent at any time.

Once consent is withdrawn by the data subject, the school will cease processing data for the specified purpose without undue delay.

If the school wishes to offer information Society Services (ISS) to pupils it will gain parental consent for any pupil below the age of 13.

7. Accountability and Governance

Data Protection Officer (DPO)

Under the UK GDPR, it is mandatory for schools to designate a Data Protection Officer (DPO). The DPO's minimum tasks are defined in Article 39:

- To inform and advise the organisation and its employees about their obligations to comply with the UK GDPR and other data protection laws.
- To monitor compliance with the UK GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments, train staff and conduct internal audits.
- To be the first point of contact for the Information Commissioner's Office.

The contact details for the school's designated DPO are as follows:

Data Protection Officer, Information Governance Team

Blackpool Council, Number One, Bickerstaffe Square, Blackpool, FY1 3AH
SchoolsDPO@blackpool.gov.uk

Staff can contact the DPO if they have any queries about this policy, data protection law, data retention or the security of personal data. The DPO can also be contacted directly if members of staff have any concerns that this policy is not being adhered to.

Record of Processing Activities (ROPA)

The school is required to maintain records of activities related to higher risk processing of personal data.
The school maintains a ROPA in conjunction with their DPO. All employees are required to notify their data protection lead or DPO before they embark on any new processing activities so they can be adequately recorded on the school's ROPA.

Workforce Training

The school is committed to providing data protection training to all staff as part of their induction process and will issue regular refresh training throughout the course of their employment or in the event of any changes in data protection law. The school will retain a record of this training programme and this will be made available to the Information Commissioner's Office on request.

Data Protection Impact Assessments (DPIAs)

Data protection impact assessments (DPIAs) are a tool which can help the school identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA allows organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.

The school will complete a DPIA for certain listed types of processing, or any other processing that is likely to result in a high risk to individuals' interests. Therefore, staff must consult the relevant persons or DPO before they embark on any new processing that could be regarded as being high risk to an individuals' interests. If required, the DPO will assist members of staff completing the school's DPIA template.

The school has a supplementary DPIA Procedure, which assists employees in understanding the purpose of a DPIA and when/how to complete one.

Contracts

Whenever a controller uses a processor, it needs to have a written contract in place. This is important so that both parties understand their responsibilities and liabilities. The school commits to including the following compulsory details in its contracts:

- 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; and
- The obligations and rights of the controller.

The school has a supplementary Procurement Procedure, which outlines its commitment in more detail.

8. Individual Rights

Right to be Informed

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the UK GDPR. It is called 'privacy information' and the school will issue privacy notices in relation to pupil data, workforce data and governor data. The school will endeavour to issue these notices on induction and also make them available on the school's website throughout the data subject's school life.

Right of Access

Individuals have the right to access their personal data (commonly known as subject access) and supplementary information about the processing of their data. The right of access allows individuals to be aware of and verify the lawfulness of the processing of their personal data. The information that can be requested includes:

- Confirmation that their personal data is being processed.
- Access to a copy of the data.
- The purposes of the data processing.
- The categories of personal data concerned.
- Who the data has been, or will be, shared with.
- How long the data will be stored for.
- The source of the data, if not the individual.
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

'Subject access' requests can be submitted to the school office and should contain the name of the data subject, a correspondence address and a description of the information requested. The school will provide the information without delay and at the latest within one month of receipt of the request. The school will not apply a fee to requests unless the request is manifestly unfounded or excessive. The school will take reasonable steps to verify the identification of the applicant and if the applicant wishes to request a review of the school's decision, the process for doing so will be clearly outlined in the response issued.

The school has a supplementary Subject Access Procedure, which outlines the process for receiving and responding to a request in more detail.

Individual Rights

The UK GDPR also empowers individuals with the right to rectification, erasure, right to restrict processing, data portability, right to object and rights in relation to automated decision making or profiling. Any requests should be passed to the school's Data Protection Lead as soon as received, who will consider the request alongside the DPO.

9. Data Security

Principle f of the UK GDPR states data should be processed in a manner that ensures appropriate security of the personal data. This means that the school must have appropriate security to prevent the personal data it holds being accidentally or deliberately compromised. Particular attention will be paid to the need for security of sensitive personal data.

Manual data will be stored where it is not accessible to anyone who does not have a legitimate reason to view or process that data. Staff should carefully consider whether they need to take any manual data offsite before doing so and record instances where any 'special categories of data' is taken offsite. The following measures must be taken by staff in relation to electronic data:

- Portable electronic devices, such as laptops, ipads and hard drives that contain personal data are stored in a locked cupboard or draw.
- Encryption software is used to protect all portable devices and removable media that contain personal data, such as laptops and USB devices.
- Passwords must meet appropriate security standards, be changed at regular intervals and must not be divulged to any other persons.
- Where personal data is shared with a third party, staff should carry out due diligence and ensure the data is sent in a secure manner or appropriate measures are taken to mitigate the risk of individuals being identified.
- When sending personal data to a third party, staff must carefully check the recipient and their contact details.
- Where personal devices are used to access organisational email accounts, staff should ensure appropriate passwords are applied to the device.
- Staff should not open links when emails are received from unknown recipients or the emails appear suspicious.
- Personal data must be stored in a secure and safe manner, with careful consideration made to who can access the data.

10. Breach Reporting

The UK GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. Where feasible, the school must do this within 72 hours of becoming aware of the breach. It is essential that **all members of staff make the relevant persons aware of any potential breaches of data protection without undue delay.** This includes all losses, thefts or inadvertent disclosures of personal data. It also includes the loss or theft of any device that holds personal data.

The relevant persons will then follow the breach procedure in conjunction with the DPO. An investigation will be conducted to confirm whether or not a personal data breach has occurred. If a breach has occurred the DPO will advise the school on whether it is required to notify the Information Commissioner and the data subjects affected.

The school has a supplementary Personal Data Breach Procedure, which all staff should familiarise themselves with.

11. Data Retention

Principle e of the UK GDPR states data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Data will only be retained for the specified period outlined in the records management schedule that the school has adopted and will be destroyed in a secure manner thereafter.

The school has a Records Management Policy which outlines its commitment to adhering to this principle and contains the school's model retention schedule.

12. Data Accuracy and Limitation

Principle d of the UK GDPR states data shall be accurate and, where necessary, kept up to date The school will issue regular reminders to staff and parents/carers to ensure that personal data held is up to date and accurate. Any inaccuracies discovered will be rectified and if the inaccurate information has been disclosed to a third party; the recipients will be informed of the corrected data.

The school will only collect personal data for specified, explicit and legitimate reasons. The school will explain these reasons to the individuals in the school's privacy notices. If the school wants to use personal data for reasons other than those given when it first obtains it, it will inform the individuals concerned before it does so, and seek consent where necessary. Staff must only process personal data where it is necessary to do so in their jobs.

13. Information Requests

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request. The school will adhere with 'subject access' requests as outlined in Section 7.2 of this policy.

Personal data will only be disclosed to third party organisations or individuals for whom consent has been given to receive the data, or organisations that have a legal right to receive the data without consent being given e.g. examination boards.

Requests for personal data by the Police or other bodies with law enforcement powers (e.g. HMRC), will usually only be considered when accompanied by an appropriate data protection exemption. The request should contain details of the applicant, the purpose of the request and the section of the legislation the information is being requested under. This will allow the DPO to make an informed decision as to whether the request is proportionate for the purpose requested, against the rights of the data subject.

If requests are received from parents/carers for the names of pupils in their class (e.g. for Christmas card or birthday invites), only first names will usually be released, however the school reserves the right to refuse any req

14. Biometric Data

Where the school uses pupils' biometric data as part of an automated biometric recognition system, it will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it. Parents/carers and pupils have the right to choose not to use the school's biometric system(s) and the school will provide alternative means of accessing the relevant services for those pupils. Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and the school will ensure that any relevant data already captured is deleted.

Where staff members or other adults use the school's biometric system(s), the school will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service should they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

15. Document Control

Document owner:	Jonathan Pickup
Document number:	Schools - r - 03
Document category:	Procedures
Document location:	365 IG Team / Schools / Policies & Procedures

Record of Amendments:

Date	Version	Amended by	Description of changes
02.04.2019	0.1	Head of IG/DPO	First Draft
14.05.2019	1.0	Head of IG/DPO	Final Version
15.09.2021	1.1	Information Governance Specialist	Reviewed Version