St John Baptist Church in Wales

GDPR Data Protection Policy

DATA PROTECTION POLICY V1.0

Document Information

Version:	Version 1.0
Status:	FINAL
Date:	25.11.2019

Signed by Chair of Governors on behalf of the Governing Body……

Signed by Headteacher……..

Date: September 2019

Contents

Section	Heading	Page
1.	Introduction	3
2.	Legal Requirements	3
3.	Scope	4
4.	Links to other policies	5
5.	General Data Protection Regulation – Principles	5
6.	Information Rights	8
7.	Roles & Responsibilities	9
8.	Record of Processing Activity	11
9.	Data Protection Impact Assessment	12
10.	Breaches of Personal Data	12
11.	Data Protection Complaints	13

App I	Definitions	14
App II	Information Governance	16

1. INTRODUCTION

1.1 The School needs to collect personal and sometimes sensitive information to perform its functions and to comply with the requirements of Laws and Regulations. In addition, the School is also responsible for sharing information in accordance with requirements placed upon it.

1.2 No matter how it is collected, recorded and used, information must be dealt with properly to ensure compliance with Data Protection legislation.

1.3 Processing information in a lawful manner is extremely important to the School and demonstrates clear accountability and transparency to individuals.

1.4 This Policy provides an overview of the School's governance arrangements in respect of managing the information that it processes and it applies to all workers. It includes organisational measures and individual responsibilities which aim to ensure that the School complies with the Data Protection legislation and respects the rights of individuals.

2. LEGAL REQUIREMENTS

General Data Protection Regulation (GDPR)

2.1 The General Data Protection Regulation 2016 (GDPR) is EU wide legislation.

2.2 The regulation governs how information about people (personal data) should be treated. It also gives rights to the individuals whose data is being processed and held. It applies to any data that relates to "an identified or an identifiable natural person (data subject)".

2.3 The GDPR is fully retrospective, in that it applies to information collected prior to the regulation coming into force.

2.4 The GDPR is enforced by the Information Commissioner. There are a number of tools available to the Information Commissioner for taking action to change the behaviour of organisations that process personal information where the law is broken. They include criminal prosecution, non-criminal enforcement and audit. The Information Commissioner also has the power to serve monetary penalties:

- Tier 1 - €10M or 2% of worldwide annual turnover for administrative errors e.g. failing to notify a breach when required to do so.

- Tier 2 - €20M or 4% of worldwide annual turnover for failing to comply with the principles or breaching data subject rights e.g. failing to keep personal information secure, failing to comply with a request for personal information.

Data Protection Act 2018 (DPA)

2.5 The DPA 2018, replaces the Data Protection Act 1998. The Act aims to modernise data protection laws to ensure they are effective in years to come.

2.6 The Act has a part dealing with processing that does not fall within EU law. It applies GDPR standards but it has been amended to adjust those that would not work in the national context.

3. SCOPE

3.1 This Policy applies to all staff employed by the School, and to external organisations or individuals working on the School's behalf.

3.2 The Policy also applies to personal data processed by Governors when representing the School.

3.3 The Policy applies to all processing of personal data for which the School is the Data Controller. This includes:

- Personal data processed by the School
- Personal data controlled by the School but processed by a third party on the School's behalf (for example confidential waste disposal).
- Personal data processed jointly by the School and its partners (data controllers in common).

3.4 Data subjects may include, but are not limited to:

- Students/ pupils
- Parents/ carers or representatives of others
- Student/ pupil contacts
- Employees – prospective, past, present (permanent, temporary and casual etc.)
- Employee contacts
- Student teachers
- Work experience students
- Volunteers
- Service users (e.g. facilities hirers)
- Suppliers
- Vendors
- Members of the public
- Visitors
- Others with whom the School communicates

3.5 The Policy applies to all personal data regardless of the media in which it is held including electronic data, CCTV, video and sound recordings and data held in physical

format (e.g. paper records).

4. LINKS TO OTHER POLICIES

4.1 A suite of supporting procedures, guidance documents, toolkits and frameworks underpin this Policy. These documents form the School's Information Management Framework and help to demonstrate a commitment to accountability and transparency.

5.0 GENERAL DATA PROTECTION REGULATION - PRINCIPLES

5.1 Six key principles are noted in Article 5 of the GDPR and these effectively summarise the main responsibilities placed upon organisations. The following summarises the six principles and illustrates how the School will aim to comply with each of them:

5.2 Article 5 (1 (a)) - Personal data shall be processed lawfully, fairly and in a transparent manner

In order to comply with this principle the School will inform data subjects what it does with their personal data. This means that the School will aim to:

- Review the purpose of its processing activities and establish an appropriate lawful basis for each activity.

- The School will only process personal data where we have one of 6 'lawful bases' to do so under data protection law:
    - The data needs to be processed so that the School can **fulfil a contract** with the individual, or the individual has asked the School to take specific steps before entering into a contract
    - The data needs to be processed so that the School can **comply with a legal obligation**
    - The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
    - The data needs to be processed so that the School, as a public authority, can perform a task **in the public interest**, and carry out its official functions
    - The data needs to be processed for the **legitimate interests** of the School or a third party (provided the individual's rights and freedoms are not overridden)
    - The individual (or their parent/ carer, when appropriate, in the case of a pupil) has freely given clear **consent**

- For special categories of personal data, the School will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

- At the point in which personal data is collected the School will explain in a clear and accessible way:
    - What personal data is collected;
    - For what purposes;
    - Why it is needed;
    - How it is used;
    - How personal data will be protected;
    - To whom they may disclose it and why;
    - How data subjects can update their personal data that is held; and
    - How long they intend to keep it

- Tailor this information for children, staff and other groups of people as appropriate.

- Publish this information in the form of 'Privacy Notices' and these will be made available on the School's website, and where appropriate in printed formats.
    - Privacy Notices will be reviewed regularly, and should significant changes occur data subjects will be informed.

- Wherever consent is required to process personal information, the School will aim to:
    - make the request for consent prominent and 'granular' (separate consent for separate things);
    - not use pre-ticked boxes or any other type of default consent;
    - ask people to positively opt in and provide clear instructions regarding withdrawal of consent;
    - ensure that individuals can refuse to consent without detriment; and
    - specify the purpose for processing.

5.3 Article 5 (1 (b)) - Personal data shall be collected for specified, explicit and legitimate purposes

In order to comply with this principle the School will verify that the processing is necessary for the relevant purpose, and ensure that it is satisfied that there is no other reasonable way to achieve that purpose.

5.4 Article 5 (1 (c)) - Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

5.5 Article 5 (1 (d)) - Personal data shall be accurate and, where necessary, kept up to date

5.6 Article 5 (1 (e)) - Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary

In order to comply with the three data quality principles above the School will:

- Obtain and process personal data only to the extent that is necessary to perform its functions i.e. personal data will be relevant to the stated purpose and adequate but not excessive.

- Ensure, as far as is practicable, that the information held is accurate and up-to-date.

- If personal data is found to be inaccurate, this will be remedied as soon as possible.

- Share personal information, such as contact details, within the School where it is necessary to keep records accurate and up-to-date.

- Will retain personal data only for as long as required.

- Apply the School's Retention & Disposal guidelines.

- Keep records only for as long as required in accordance with these guidelines.

- Dispose of personal information by means that protect the right of those individuals i.e. shredding, confidential waste.

5.7 Article 5 (1 (f)) - Personal data shall be processed in a manner that ensures appropriate security of the personal data

In order to comply with this principle the School will take appropriate steps to safeguard all personal data it holds and minimise the risk of loss, wrongful access or improper use. This means that the School will:

- Control access to personal data so that staff and other people working on school business can only see such personal data as is necessary for them to fulfil their duties.

- Require all school staff, and others who have access to personal data in the course of their work to complete basic data protection training, supplemented as appropriate by procedures and guidance relevant to their specific roles.

- Set and monitor compliance with security standards for the management of personal data as part of the School's wider framework of information security policies and procedures.

- Provide appropriate tools for staff and others to use and communicate personal data securely when working away from the main office environment when their duties require this.

- Take all reasonable steps to ensure that all suppliers, contractors, agents and other external bodies and individuals who process personal data on behalf of the School enter into a Data Processor Agreement and comply with auditable security controls to protect the data.

- Take all reasonable steps to ensure that information is not transferred outside

the European Economic Area, without verifying that the organisation processing the personal data has provided adequate safeguards.

- Develop and maintain Information Sharing Agreements (in keeping with Welsh Government's Wales Accord on the Sharing of Personal Information framework) with partner organisations and other external bodies with whom we may need to share personal data to deliver shared services or joint projects to ensure proper governance, accountability and control over the use of such data.

- Make appropriate and timely arrangements to ensure the confidential destruction of personal data in all media and formats when it is no longer required for School business.

6.0 INFORMATION RIGHTS

6.1 The GDPR provides certain rights to individuals. The School is committed to ensuring individuals can freely exercise their rights and has procedures in place to ensure staff are aware of and can respond to requests of this nature. Below is a summary of those key rights:

i. Right to be informed

As explained in detail in section 5.2 above, the School must provide concise, transparent, intelligible and easily accessible information about the processing of personal data to individuals by means of a document known as a Privacy Notice. This must be written in clear plain language and clearly set out how personal data is processed within the School and the purposes for which it is used.

ii. Right to access

This allows the individual to ask the School if it holds personal information about them, what it uses the information for and to be given a copy of that information.

iii. Right to correct incorrect information (rectification)

This allows the individual to ask the School to have their personal information rectified if it is inaccurate or incomplete.

iv. Right to erasure

This allows the individual to ask the School to have their personal information deleted or removed if there is no compelling reason for its continued use. This is not an absolute right and only applies in certain (limited) circumstances.

v. Right to restrict the use of your information

This gives the individual the right to ask the School to block or stop using their personal information if its continued use causes them substantial and unwarranted damage or distress. This is not an absolute right and only applies in certain limited circumstances.

vi. Right to portability

This right allows the individual to ask the School for an electronic copy of their personal information in a readable format so that they may provide it to another organisation or service provider. The right to portability applies in certain limited circumstances.

vii. Right to object to the use of your information

This right allows the individual to object to the School processing their personal information:

- where processing is based on legitimate interests of the performance of a task in the public interests/ exercise of official authority
- for direct marketing purposes
- profiling (any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual)
- research purposes

viii. Rights in relation to automated decision making and profiling

This right enables the individual (in some circumstances) to object to the School making significant decisions about them where the decision is completely automated and there is no human involvement.

7. ROLES AND RESPONSIBILITIES

7.1 To ensure compliance with data protection legislation all staff must understand their roles and responsibilities when managing personal data. This creates clear lines of leadership, accountability and governance, as well as promoting a culture where personal information is valued and protected.

7.2 Specific roles, responsibilities and governance arrangements have been established in line with data protection legislation.

Key roles/ groups are as follows:

i. Data Protection Officer (Statutory Post)

Article 37 of the GDPR requires that all public authorities/ bodies shall appoint a Data Protection Officer (DPO). Under Section 3 (1) (a) (i) Schedule 1 of the Freedom of Information Act, maintained schools and further and higher education institutions are defined as public authorities.

The main tasks of the DPO as outlined in Article 39 of the GDPR is to:

- **inform and advise** the controller and the employees who carry out processing of their data protection obligations;
- monitor compliance with the GDPR and other data protection laws, and the controllers' data protection policies;
- raise awareness and deliver training;
- undertake compliance audits; and
- act as a point of contact for the Information Commissioners Officer.

The Council's Principal Information Management & Data Protection Officer is the designated DPO for the School. The DPO provides interpretation, advice and support on complex information governance and information compliance issues.

ii. Schools Data Protection Working Group

The Schools Data Protection Working Group (SDPWG) consists of a representative group of Head Teachers/ Data Protection Leads and key Local Authority staff whose purpose is to support and drive the broader Data Protection agenda within RCT Schools. It specifically covers compliance with the GDPR and the Services within the Service Level Agreement (SLA) between RCTCBC and Schools.

The primary role of the group is to:

- Support the Local Authority in evaluating and assessing the current position within Schools in relation to data protection compliance.
- Support the development and implementation of a Schools 'Data Protection' compliance plan.
- Act as a conduit for all Schools, communicating issues in relation to data protection that require consultation, discussion and clarification.

iii. Information Asset Owners (IAO)

The role of the IAO is assigned to someone who will have ultimate ownership and accountability of information systems and assets held within the School. This is typically identified at a Head Teacher level.

IAO's have responsibility for making sure that information systems and assets are handled and managed appropriately. This means making sure that personal information is properly protected, and where personal information is shared, that proper confidentiality, integrity and safeguards apply.

IAO's are responsible for ensuring that their staff process personal data in compliance with the 6 principles of the GDPR (as set out earlier in Section 5 of the Policy).

iv. Link Governor

The School has a designated Link Governor for Data Protection, who acts as the link/ liaison between the governing body in relation to data protection matters.

v. Data Protection Lead

The School has a designated Data Protection Lead, who is responsible for data protection compliance within the School.

The primary role of the Data Protection Lead (DPL) is to promote and improve good data protection practice within the School. The DPL will be the main point of contact within the School for data protection matters, liaising directly with the Local Authority's DPO for advice and guidance.

vi. All Data Users

Almost every member of staff within the School handles and manages personal information as part of their day-to-day role and as such they all have an important role in effectively managing information throughout its lifecycle i.e. from the time it's created, to the time it's no longer needed and disposed of.

Individual Responsibilities:

- All data users must comply with this Policy. Failure to comply may result in disciplinary action which could lead to dismissal.
- Take part in relevant training and awareness to support compliance.
- Take all necessary steps to ensure that no breaches of personal data result from their actions.
- Report all suspected information security breaches promptly so that appropriate action can be taken to minimise harm.

8. RECORDS OF PROCESSING ACTIVITY

8.1 The GDPR contains explicit provisions regarding the need for organisations to document their processing activities. In order to discharge this key responsibility, the School has in place Data Protection Registers (DPRs). The DPRs document the following for each processing activity:

- purpose for processing;
- legal basis for processing;
- arrangements in respect of information sharing (with both internal and external partners);
- retention requirements;
- information required for privacy notices;

- records of consent;
- controller-processor contracts;
- the location of personal data;
- Data Protection Impact Assessment reports; and
- Records of personal data breaches.

8.2 Each DPR will be subjected to regular review.

9. DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

9.1 The School will apply 'privacy by design' principles when developing and managing information systems and processes involving personal data.

9.2 Specifically the School will:

- Undertake proportionate DPIA's to identify and mitigate data protection risks at an early stage of a project where new technology is being deployed or the processing is likely to result in a high risk to the rights and freedoms of individuals.
- Collect, disclose and retain the minimum personal data for the minimum time *necessary* for the purpose (i.e. adopt data minimisation).
- Anonymise personal data wherever necessary and appropriate, for instance when using it for statistical purposes.

10. BREACHES OF PERSONAL DATA

10.1 The GDPR introduces a duty on all organisations to report certain types of personal data breaches to the relevant supervisory authority (Information Commissioner). This must be done within 72 hours of becoming aware of the breach, where feasible.

10.2 If the breach is likely to result in a high risk of adversely affecting individual's rights and freedoms, the organisation must also inform those individuals without undue delay.

10.3 The School has robust breach detection, reporting and investigation procedures in place that aim to ensure that:

- data breach events are detected, reported, categorised and monitored consistently;
- incidents are assessed and responded to appropriately;
- action is taken to reduce the impact of disclosure;
- mitigation improvements are put in place to prevent recurrence;
- serious breaches will be reported to the Information Commissioner; and
- lessons learnt are communicated and actions to help prevent future incidents are agreed and monitored.

11. DATA PROTECTIONS COMPLAINTS

11.1 The School is committed to dealing effectively with any complaints or concerns individuals may have about the way in which the School processes personal information. Any complaints about the School's processing of personal data and rights under the Regulation will be dealt with in accordance with this Policy and the School's Complaints Policy.

11.2 Data protection complaints may be addressed directly to the School's Data Protection Lead (email/address below), or may be submitted by any of the means highlighted in the School's Complaints Policy.

FAO: Data Protection Lead
St John Baptist (CiW) High School
Glan Road
Aberdare
CF44 8BW
e-mail: Office@StJohnBaptist.co.uk

11.3 The GDPR does not set out a specific complaints regime for data protection issues. However individuals do have a right to request that the Information Commissioner make an assessment of compliance of particular circumstances with the GDPR.

The Information Commissioner's Office
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire,
SK9 5AF

www.ico.org.uk Telephone: 0303 123 1113

11.4 The School will respond promptly and fully to any request for information about data protection compliance made by the Information Commissioner.

Appendix I

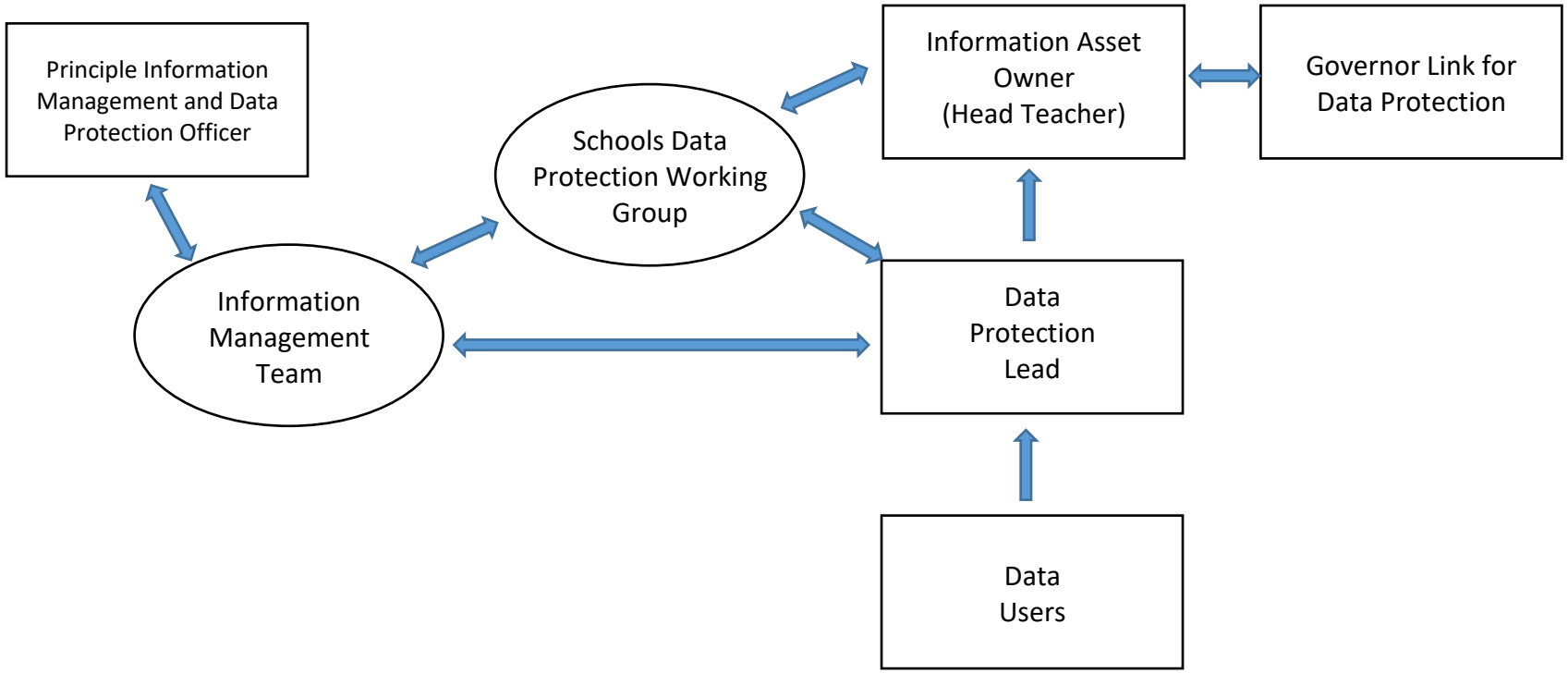
DEFINITIONS

GDPR	General Data Protection Regulation 2016
DPA	Data Protection Act 2018
Personal data	Personal data is defined as - any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, address, date of birth, 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.
Special categories of data	Formerly known as sensitive data, special category data is more sensitive, and so needs more protection. The categories are as follows: • racial or ethnic origin, • political opinions, • religious or philosophical beliefs, • trade union membership • genetic data, • biometric data for the purpose of uniquely identifying a natural person, • data concerning health • data concerning a natural person's sex life or sexual orientation
Criminal Convictions	Whilst not classified as special category data by the GDPR, the processing of personal data relating to criminal convictions and offences carries specific instructions under Article 10 of the GDPR and also Schedule 1 of the DPA.
Data Subject	A Data Subject is the technical term for a living individual to whom the personal data relates. Within the School this could be a pupil or an employee (for example).
Data Controller	A Data Controller is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Controllers are the main decision makers and must make sure that the processing of data complies with data protection law.

Joint Data Controller	The term jointly is used where two or more persons/ organisations act together to decide the purpose and manner of any data processing.
Data Controller in common	The term applies where two or more persons/ organisations share a pool of personal data that they process independently of each other.
Data Processor	A Data Processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller and in accordance with their instructions.
Processing	The definition of 'processing' is very wide and covers virtually any action associated with personal data including (but not limited to) collecting, recording, organising, structuring, storing, using, adapting, altering, analysing, combining, disclosing, disseminating and deleting the data.
Data User	The term data user applies to any member of staff, contractor or third party who processes personal information held by, or on behalf of the School.
Information Commissioner	The Crown appointed person (and department) responsible for the implementation and the policing of GDPR, DPA and the Freedom of Information Act 2000. He/ she has the authority to both investigate and prosecute on behalf of any individual who believes that their Personal Data is not being handled in accordance with the legislation.
ICO	Information Commissioner's Office

Appendix II

Information Governance Flowchart



Document Control

Policy	GDPR
Title	GDPR Data Protection Policy
Author	C Loveridge
Owner	C Loveridge
Review date	This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Document Approvals

This document requires approval of the School Data Protection Working Group:

Version Control

Version No	Date Approved	Valid From Date	Valid To Date	Changes Made
1.0	25.11.2019	25.11.2019	25.11.2020	Document created