

St John Baptist (Southend) CE Primary School



DATA PROTECTION POLICY

Agreed: Dec 2016

Review Date: Dec 2019

By: Curriculum and Pupil Welfare Committee

1. Introduction

In collecting, processing, sharing and disposing of personal information relating to living individuals, St John Baptist School is bound by the Data Protection Act 1998.

The Information Commissioner's Office enforces the Act, issues relevant guidance and registers personal data sets held by any organisation.

As a data controller, St John Baptist School must register itself with the Information Commissioners Office (ICO) annually.

This document sets out St John Baptist School policy for compliance with the Data Protection Act (DPA).

The objective of this policy is to set out the rules and conditions for St John Baptist School (including all it's staff) to follow when obtaining and using information about individuals.

The Eight Guiding Principles

St Johns Baptist School is a registered Data Controller under the Act and will comply with the eight principles below:

- 1 Personal data shall be processed fairly and lawfully.
- 2 Personal data shall be obtained for specified and lawful purposes.
- 3 Personal data shall be adequate, relevant and not excessive.
- 4 Personal data shall be accurate and up to date.
- 5 Personal data shall only be kept as long as necessary.
- 6 Personal data shall be processed in accordance with the rights of data subjects under the Act.
- 7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing and against accidental loss, damage or destruction of personal data.
- 8 Personal data should not be transferred to a country outside the European Economic Area (EEA) unless that country has an adequate level of protection.

The Act creates a single framework for access to personal information (principle 6) about living individuals held in both paper and electronic form.

See Schools guidance on what to do when a Subject Access Request (SAR) is received.

2. Differences in data sets

Personal and Personal Sensitive data is any information – held manually or electronically – which relates directly to a living individual.

Personal Data-

This can include but is not limited to:

- Name and Address
- Contact Number
- E-mail address
- Date of Birth
- Qualifications
- Income level
- Employment history
- Bank Details

Sensitive Personal Data-

This includes data under the following headings:

- Race or ethnic origin
- political opinion/s
- religious or other beliefs
- trade union membership
- physical or mental health or condition
- sexual orientation
- the commission or alleged commission of offences, court sentences or allegations under investigation

3. Roles and Responsibilities

Head of School

- Responsible for ensuring all senior staff and the school is compliant with the data protection act

School Business Manager

- Maintaining the notification of registration for St Johns Baptist School with the Information Commissioner's Office on an annual basis

Head of School & School Business Manager

- Providing guidance to ensure all staff are aware of their data protection responsibilities under the act

- Responsible for managing and reporting data breaches to the schools data protection advisor
- Providing guidance to process Subject Access Requests made under the act and Freedom of Information requests
- Ensuring appropriate and adequate training is available to staff
- Ensure staff are compliant with this policy and any associated procedures

All Staff

- All staff have a responsibility to abide by the principles of the Data Protection Act. Any breach of this policy could lead to disciplinary action being taken.

4. Processing Personal Data

Employees of St John Baptist School, when working with personal data, will adhere to the following:

- Only collect data necessary to carry out the purpose that the task relates to
- Respond to requests for access to personal data within 40 calendar days (See Schools Guidance)
- Treat all personal information with equal respect for confidentiality and security whether in written, spoken or electronic form.
- Seek consent to the sharing of personal or sensitive data where applicable, unless doing so would interfere with other statutory requirements, such as law enforcement, or legislation that permits such sharing.
- Only retain personal data for a specified time period defined by the Schools Retention Schedule. (See specific schools guidance on retention)
- Not delay data sharing where it is necessary to protect the vital interests of any individual.
- Only use third parties to collect and process schools data where they can ensure confidentiality of schools data
- Seek approval from senior management before disclosing information for research purposes

5. Fair Processing and Privacy Notices

Fair Processing

Principle 1 of the data protection states that all personal data will be processed fairly

and lawfully. The data protection Act does not define fair processing, but it does say that, unless relevant conditions or exemptions apply personal data must be processed fairly.

St John Baptist School will include a fair processing statement on data collection forms (paper or electronic) which explains why the data is being collected and for what specific purpose/s. Having this statement means that any individual will be able to read this before the complete a form and therefore will know exactly what their data is being collected for.

The statement will include what the data is being used for, whether the data will or may be used for other purposes, the identity of the data controller (the school) and any extra information which in the circumstances will help the individual to understand how their data is used in line with data protection.

Privacy Notices

A Privacy Notice is a written statement that will explain to individuals how St John Baptist School will process their data. This notice differs somewhat to a fair processing notice as it should be openly accessible to the public.

In general terms, a Privacy Notice should tell individuals the following about St John Baptist School:

- Who we are
- Where we are based in the UK
- What we are going to use their data for
- Who we will share individual's data with
- Individuals Rights to accessing their own data
- How we will keep individuals data secure and protected

A privacy notice should be genuinely informative and clear so St John Baptist School can be transparent and give individuals reassurance that they can trust the school with their personal data.

A privacy must be visible and easily accessible on the school's website

6. Information Sharing

The school will share personal and personal sensitive information on a daily basis as much of the sharing completed is governed by legislation. Sharing of personal and personal sensitive data must be protected under principle 7 of the data protection act. (protecting data when sharing)

See the schools IT policy for more information on protecting information electronically and the records management policy for handling paper documentation.

7. Subject Access Requests

Individuals have a right of access to information about themselves that includes factual information, expressions of opinion, and the intentions of St John Baptist School in relation to them, irrespective of when the information was recorded.

St John Baptist School will disclose any information they hold on a individual (applying any necessary exemptions) within 40 calendar days of receiving a valid Subject Access Request.

See Subject Access Request guidance for details

(For help and advice in responding to an Subject Access Request, contact the schools data protection officer)

8. Fees

St John Baptist School reserves the right to charge the statutory fee for Access to Information Requests:

- Standard Subject Access Requests- £10
- Educational Record Request the fee will depend on the number of pages of information supplied. (For more information ask at the schools business manager)
- Freedom of Information Request- No Fee

9. Appeals & Role of the ICO

In the event of a complaint or challenge regarding a subject access request response, the initial request, decision audit trail, correspondence and information released will be reviewed independently of the original decision maker.

If the requestor is dissatisfied with the appeal outcome they may seek an independent review by the Information Commissioner.

The Information Commissioner has the authority to demand disclosure.

The Information Commissioner is an independent official appointed by the Crown to oversee the Data Protection Act.

In the first instance however the Information Commissioner will usually expect that individuals will have taken the matter up first with the School.

St John Baptist School will comply with all notices and guidance issued by the Information Commissioner.

10. Freedom of Information Requests

The Freedom of Information Act 2000 (FOIA) allows anyone to request information from a school. Any non confidential information held by St John Baptist School is eligible for release. However, a limited number of exemptions may be applied to protect categories of information.

The Act requires that all requests must be in writing (to include faxes and e-mails). Requests must state clearly what information is required and must provide the name of the person with an address for correspondence.

See Freedom of Information guidance for details

(For help and advice in responding to an FOI request, contact the schools data protection officer)

11. Dealing with breaches of the Data Protection Act

St John Baptist School holds personal and sensitive data relating to employees, children and their families, etc.

Every care must be taken to protect personal data and to avoid a data protection breach. In the unlikely event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible.

What is a data breach?

Inadvertent breaches of confidentiality can occur. The following are examples:

- Reading confidential files when there is no requirement to do so
- Giving excessive information out when less would suffice
- Sending information in error eg.to a wrong email address
- Files/records removed from the office and lost
- Unencrypted devices used and lost containing personal/sensitive details
- Information that hasn't been redacted correctly before publishing

Known breaches in confidentiality must be reported to the Schools Business Manager immediately so it can be recorded and a formal investigation carried out.

What to do when a breach occurs:

There are four elements in dealing with a data breach. These are:

1. Containment and recovery
2. Assessment of ongoing risk
3. Notification of breach
4. Evaluation and response

See the schools data breach guidance so you know what to do in the event of a data breach

12. Training

It is the aim of St Johns Baptist School to train all staff so they are fully informed of their obligations under the Data Protection Act and aware of their responsibilities.

13. Confidentiality

The School intends that personal data must be treated as confidential. All staff must comply with the Schools Data Protection Policy, Information Security Policy.

All School Staff must sign and agree to the data protection Policy

14. What happens if this policy is breached?

Failure to adhere to this or any related policy, could lead to disciplinary action

15. Policy Authorisation

Role	Name
Data Protection Officer for Schools	Zoe Horsewell
Head of School	Caroline Phillips
School Business Manager	Joyce Joseph
Chair of Governors	Andrea Blower