St. John's C. of E.

Blackpool's First Free School 1817

Data Protection Policy

Last updated: April 2024

Table of Contents

Aims

St Johns C of E Primary School aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) 2018.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

Legislation and guidance

This policy meets the requirements of the GDPR Regulation 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on GDPR and the ICO's code of practice for subject access requests.

The regulation provides a balance between an individual's rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It aims to protect the rights of individuals about whom data is obtained, stored, processed, retained, deleted or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration and disclosure.

Definitions

Personal data
Any information relating to an identified, or identifiable, individual. This may include the individual's:

- Name (including initials)
- Identification number
- Location data
- Online identifier, such as a username

It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural, or social identity.

Special categories of personal data
Personal data, which is more sensitive and so needs more protection, including information about an individual's:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetics
- Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes
- Health – physical or mental
- Sex life or sexual orientation

Processing
Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual

Data subject
The identified or identifiable individual whose personal data is held or processed.

Data controller
A person or organisation that determines the purposes and the means of processing of personal data.

Data processor
A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

Personal data breach
A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

The Data controller
St Johns C of E Primary School processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller. Our school delegates the responsibility of data controller to the employees of the school.

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

Roles and responsibilities
This policy applies to all staff employed by St Johns C of E Primary School and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Governing Board
The Governing Board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

Data Protection Officer
The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governors and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Our DPO is Sheryl Cardwell and is contactable via dpo@st-john@blackpool.sch.uk

Data Protection Principles

The GDPR is based on data protection principles that our school must comply with.
The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

Collecting personal data

<u>Lawfulness, fairness and transparency</u>

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) 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, we will also meet one of the special category conditions for processing which are set out in article 9 of the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

<u>Limitation, minimisation and accuracy</u>

We will only collect personal data for specified, explicit, and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.
When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's Records Management and Retention Schedule.

Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent when necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Subject access requests and other rights of individuals

Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This 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, or if this isn't possible, the criteria used to determine this period
- 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 should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request, they must immediately forward it to the DPO. It is important to note that subject access requests can be submitted verbally or through written means.

Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information. `

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

Other data protection rights of the individual

In addition to the right to make a subject access request and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the DPO.

Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school grounds or whilst on Trips and Visits.

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- Within the school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of the school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school websites or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only process personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law
- Complete privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrate data protection into internal documents including this policy, any related policies and privacy notices
- Regularly train members of staff on GDPR legislation, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conduct reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where possible, staff will not use their personal laptops or computers for school purposes. All necessary members of staff are provided with their own electronic device (laptop, chromebook etc.), a secure login and password, and every computer regularly prompts users to change their password.
- If staff need to use their personal laptops for school purposes, particularly if they are working from home, they will bring their device into school before using it for work to ensure the appropriate software can be downloaded and information encrypted.
- Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key The person taking the information from the school premises accepts full responsibility for the security of the data. (see Acceptable Use agreement and Confidentiality Policy).
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops, and other electronic devices. Staff and pupils are required to change their passwords at regular intervals. Two-factor authentication is encouraged where possible.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices. Cloud-based storage is encouraged.
- Staff, pupils or governors should not store personal information on their personal devices. Staff should use their own devices to do, or obtain prior consent from the ICT Support Team, should this it be required for specific activities. Governors must adhere to the same security procedures as for school owned equipment for managing any personal information.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with GDPR regulation.

Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

Training

Data protection will form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed every 2 years and shared with the governing board.

Links with other policies

This data protection policy is linked to our:

- Freedom of Information Policy
- Confidentiality Policy
- Acceptable Use Agreement
- Records Management and Retention Schedule
- Privacy Notices

These policies are also designed to protect personal data and can be found at www.stjohnsblackpool.co.uk

Appendix 1

Responsibility

The overall responsibility for breach notification is Sheryl Cardwell. They are responsible for ensuring breach notification processes are adhered to by all staff and are the designated point of contact for personal data breaches. In the absence of Sheryl Cardwell, please contact Jill Hicks.

Data Protection Officer (DPO)

The schools Data Protection Officer details are as follows:
Data Protection Officer: Sheryl Cardwell
Address: C/O St Johns Primary School
Email: dpo@st-john@blackpool.sch.uk
Telephone:07714 651415

Reporting and recording a data breach

Data breaches or near misses may be identified as part of everyday business and may be identified by the office at the first point of contact, by a parent or pupil or by a third party.

What is a data breach?

Personal data breach is a security incident that has affected the confidentiality, integrity or availability of personal data. Examples of data breaches are:

- Loss or theft of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- "Blagging" offence where information is obtained by deceiving the organisation who holds it

Human error is the most common cause of data breach and may include:

- Theft of loss of paperwork
- Data posted to incorrect recipient
- Data sent by email to incorrect recipient
- Failure to redact personal / sensitive recipient

Reporting a breach

If you suspect or know a personal data breach has occurred then you must complete an online data report breach form, which is accessible by via the school shared Google Drive.

This notification will automatically be referred to the DPO for investigation. Data breach reporting is encouraged through the school and employees should seek advice if they are unsure whether a breach should be reported.

The school also encourage near misses to be reported via the data breach form, so that the school can identify areas for improvement within the organisation and make improvements. Once reported you should take no further action in relation to the breach.

Notifying others

If the data breach is likely to result in the rights and freedoms of individuals being put at risk and have a significant detrimental effect of them then the Information Commissions Office (ICO) need informing.

Examples of where the breach may have a significant effect includes:

- Potential or actual discrimination
- Potential or actual financial loss
- Potential or actual loss of confidentiality
- Risk of physical safety or reputation
- Exposure to identity theft
- Exposure to the private aspect of an individual's life becoming known to others

The ICO should be notified without undue delay and where possible within 72 hours of being aware of the data breach. If the school are unsure of whether the breach should be reported or not the assumption will be to self-report.

If the breach is identified as high risk then the individual(s) whose rights and freedoms have been affected will without undue be notified of the data breach.

On occasions the school may need to consider if other third parties need to be notified of the data breach. These may include, parents, local authority, insurers and police.

Assessing the data breach

Upon receiving the initial data breach notification, the school will notify the DPO who will decide how best to deal with the case. In the majority of instances, a formal investigation will be required to establish the scope of the breach.

Containing the breach

The school will initially look to contain or stop the breach in order to minimise further loss, destruction or unauthorised disclosure of personal data. These steps might include:

- Attempting to recover any lost equipment or personal data
- Shutting down any IT systems
- Contacting the business office team and others so they are prepared for any potential inappropriate enquires about the affected data subjects
- If an inappropriate enquiry is received staff should attempt to obtain the enquirers name and contact details and confirm that they will ring the enquirer back
- If bank details have been lost or stolen contact banks directly for advice on preventing fraud
- If the breach includes any entry codes or passwords then those codes must be changed immediately and the relevant organisations and employees informed

Investigating the breach

Having dealt with containing the breach, the school will consider the risks associated with the breach. These factors will determine whether further steps need to be taken, for example notifying the ICO. These factors include:

- The type of information and how sensitive it is
- The number data subjects are affected by the breach
- The type of protection in place, i.e. encryption

- What has happened to the data?
- Whether the information could be put to any illegal or inappropriate uses
- Who and how many data subjects have been affected?
- What could the data tell a third party about the data subject
- What are the likely consequences of the data breach on the school?
- Any other wider consequences which may be applicable

The initial investigation should be completed as a matter of priority and where possible within 24 hours of the breach being discovered. A further review of the causes of the breach and recommendations on prevent future breaches will also be undertaken.

Preventing further breaches

Once the data breach has been dealt with the school will review its security processes and procedures with the aim of preventing further security breaches. In order to do so the following will be considered:

- Were the school's security measures adequate at the time of the breach
- Consider whether there was adequate staff awareness
- Consider whether a data protection impact assessment is necessary
- Consider if further data protection audits are necessary
- Update Governors of the brief following the investigation