



## GDPR - DATA PROTECTION POLICY

### 1. STATUTORY GUIDANCE

This statutory policy has been reviewed in accordance with the following guidance:

- Data Protection Act 1998
- General Data Protection Regulations (GDPR) 2018

#### 1.1 Supporting documents

The following related information is referred to in this policy:

CCTV policy  
Privacy Notice for staff  
Privacy notice for parents

#### 1.2 Terminology

**Data Subject** means an identifiable natural person 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.

**GDPR** means General Data Protection Regulations.

**Parents** includes one or both parents or a legal guardian

**Personal Data** means any information relating to a Data Subject.

**School** means St Saviour's School Ikoyi

**Special Category Data** means data which is more sensitive and 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.

### 2. INTRODUCTION

St. Saviour's School Ikoyi is committed to protecting the personal information of individuals when they use its services. This policy is to help its students and parents, understand why and how the school collects their personal information and for what purpose. The organisation's data protection standards comply with the local law:

- It follows good practice
- It protects the rights of staff, pupils, and partners (vendors, suppliers)
- It is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach



### 3. GDPR STATEMENT

The School collects and processes Personal Data of its Data Subjects including current, former and prospective students and their parents.

This processing may include obtaining, recording, storing, disclosing, destroying or otherwise using data that relates to the Data Subjects. This policy is intended to provide information about how the school uses (or “processes”) Personal Data, to ensure all such data is stored and processed accurately, securely and purposefully in a timely manner. The School shall take all reasonable steps to abide by the latest data protection legislation in accordance with this policy.

### 4. SCOPE OF THIS POLICY

This policy applies to:

- St Saviour’s School, Ikoyi
- All staff, pupils, Board members of **St Saviour’s Ikoyi**
- All contractors, suppliers and other people working on behalf of St Saviour’s Ikoyi

It applies to all data that the school holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Home addresses
- Email addresses
- Telephone numbers
- Medical records
- Employee records
- Pupil records including assessment scores, confidential information, and behavioural records amongst other things
- Any other information relating to individuals

### 5. KEY PRINCIPLES OF GDPR

The School will comply with the following principles set out by GDPR and ensure that Personal Data will be:

- Processed fairly, lawfully and in a transparent manner,
- Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes,
- Adequate, relevant and limited to what is necessary in relation to the purposes for which data is processed,



- Accurate and, where necessary, kept up to date,
- Kept in a form that permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is processed and;
- Processed in a way that ensures appropriate security of the Personal Data including protection against unauthorised or unlawful processing and accidental loss, destruction, or damage, using appropriate technical or organisational measures.

## 6. PURPOSE

The School collects, stores and processes Personal Data in order to:

- Carry out its duties and manage its day-to-day operations as a provider of education and as an employer.
- Monitor and report on Student progress
- Support Student Learning
- Safeguard Students
- Provide appropriate pastoral care
- Provide a safe and secure environment
- Fulfil the School's contractual and legal obligations.

## 7. DATA COLLECTION

The School obtains this information by asking for details to be provided through forms and other communication means including emails and letters. The school may obtain information from the Data Subject directly, or from members of staff, other students, relevant educational organisations and professionals such as doctors.

## 8. PERSONAL DATA HELD BY THE SCHOOL

St. Saviour's School Ikoyi maintains paper and electronic records of Personal Data. The School collects, stores and may share Personal Data including:

- Name, address, email and next of kin contact details
- Special Categories of Personal Data (such as race, ethnic origin, health and biometrics)
- Attendance records (such as lessons attended, number of absences and absence reasons)
- Photographs, recordings, and other images
- Unique Student number, national curriculum assessment results, test scores, assessment and prior education information
- Financial information in relation to the payment of fees
- Expression of opinion about an individual and any indication of the intentions of the School or any other person in respect of the individual.



## 9. DATE STORAGE

- These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT department, Admin Manager, or data protection officer.
- When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.
- These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:
  - When not required, the paper or files should be kept in a locked drawer or filing cabinet.
  - Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
  - Data printouts should be shredded and disposed of securely when no longer required.
- When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:
  - Data should be protected by strong passwords that are changed regularly and never shared between employees.
  - If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
  - Data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing service.
  - Servers containing personal data should be sited in a secure location, away from general office space.
  - Data should be backed up frequently. Those backups should be tested regularly, in line with St Saviour's Ikoyi's standard backup procedures.
  - Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
  - All servers and computers containing data should be protected by approved security software and a firewall.

## 10. PRIVACY NOTICE AND FAIR PROCESSING

The School will be transparent about the intended processing of data and will communicate these intentions via notifications to its Data Subjects before the processing of their data. The School will publish a Privacy Notice for Students and Parents and a separate Privacy Notice for staff, which describe why and how the School collects and uses Personal Data and provides information about individuals' rights.

## 11. LEGAL BASIS FOR PROCESSING DATA

This section provides information about the legal basis for the School to process Personal Data:

**Consent** - the Data Subject has given clear consent for the School to process their Personal Data for a specific purpose



**Contract:** - the processing is necessary for a contract the School has with the Data Subject, or because they have asked the School to take specific steps before entering into a contract

**Legal obligation** - the processing of the data is necessary for the School to comply with the law (not including contractual obligations)

**Vital interest** - the processing is necessary to protect someone's life

**Public task** - the processing is necessary for the School to perform a task in the public interest or for the school's official functions, and the task or function has a clear basis in law

**Legitimate interest** - the processing is necessary for the School's legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the Data Subject's Personal Data which overrides those legitimate interests.

## 12. HANDLING OF DATA

The scope of this policy extends to all School departments, employees, students, relevant contractors and parents who use or access the school's data assets and information systems.

Only staff with appropriate authorisations from the School have access to Personal Data, i.e. HR

The School may make use of Personal Data relating to Students and Parents in the following ways:

- **Photographs and recordings:** the School maintains a database of photographs and recordings for internal and external publications. This includes material of individuals engaged in activities and events in the interest of creating pictorial records as well as maintaining historical records. The School shall not utilise identifiable images for publications or other communication without prior consent.
- The School may use Personal Data including CCTV recordings for the purposes of crime prevention and investigation and also in connection with its obligation to safeguard the welfare of Students, staff and visitors to the School site.
- **Promotional purposes:** with prior consent from the Data Subjects, data may be used for fundraising or promotional purposes and to maintain contact with individuals including Students, Parents and alumni for development and marketing purposes
- **Authorised disclosures of Personal Data to third parties:** any information which falls under Personal Data, and is not otherwise exempt, will remain confidential and will be disclosed to third parties only with the consent of the appropriate individual or under the terms of this policy. In order to send out School publications, contact details of the individuals may need to be shared with trusted suppliers.

The School may process some Personal Data for research, statistical information and reporting. This will not identify the Student unless prior consent has been obtained.



### 13. DATA ACCURACY

- The law requires St Saviour's Ikoyi to take reasonable steps to ensure data is kept accurate and up to date.
- Most important is that the personal data is accurate, and St Saviour's Ikoyi should put maximum effort into ensuring its accuracy.
- It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.
- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Relevant staff (IT Admin and Front office Admin) should take every opportunity to ensure data is updated. For instance, by confirming pupils' details, vendor/suppliers when they call etc.
- St Saviour's Ikoyi will make it easy for data subjects to update the information which St Saviour's Ikoyi holds about them. For instance, via forms on the Website and regular check/updates communicated through the front office.
- Data should be updated as inaccuracies are discovered. For instance, if a parent can no longer be reached on their stored telephone number nor email, it should be removed from the database.
- It is the ICT department's responsibility to ensure ALL databases are checked termly to maintain accuracy.

### 14. EXEMPTIONS

There may be circumstances where the School is required either by law or other authorities such as the Police or the Local Authority Designated Office, to pass information externally.

This may include but is not limited to information which identifies individuals, information which the School reasonably believes is likely to cause damage or distress, or information which is subject to legal professional privilege or is relevant to the prevention or detection of crime.

Data may be disclosed to authorities in respect of educational records. The School is not required to disclose any Student examination scripts. The School will treat as confidential any reference given by the School for the purpose of the education, training or employment, or prospective education, training or employment of any Student.

The School shall be at liberty to disclose facts to an educational establishment, which the Student may be transferred to, is subsequently attended by the Student or to which application for a place has been made.

There may be medical circumstances under which the School's authorised staff may need to disclose data without the express consent of the individual. These circumstances may include an emergency in the School such as a medical emergency or to prevent or detect crime.



## 15. DATA TRANSFER

Personal Data transfers outside the School are carefully considered and all steps are taken to ensure the security of the data. Data is only transferred to trusted organisations who are compliant with the latest data protection legislation.

## 16. DATA RETENTION AND RECORD KEEPING

St. Saviour's School Ikoyi has a duty to retain Personal Data for a period of time for legal and other legitimate reasons. Some data will be retained following a Student's departure from the School.

The School's guidance on data retention defines the length of time for which Personal Data and records are kept.

## 17. ACCOUNTABILITY AND STAFF RESPONSIBILITIES

Data protection risks

This policy helps to protect St Saviour's Ikoyi from some very real data security risks, including:

Breaches of confidentiality. For instance, information being given out inappropriately

Failing to offer choice. For instance, all individuals should be free to choose how St Saviour's Ikoyi uses data relating to them

Reputational damage. For instance, St Saviour's Ikoyi could suffer if hackers successfully gained access to sensitive data

Everyone who works for or with St Saviour's Ikoyi has some responsibility for ensuring data is collected, stored and handled appropriately

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

The **board of management (BOM)** is ultimately responsible for ensuring that St Saviour's Ikoyi meets its legal obligations.

The **Data Protection Officer and Headteacher** Mrs Udo Ofonagoro and Mr Heaton, respectively are responsible for:

- Keeping the board updated about data protection responsibilities, risks and issues.
- Approving any data protection statements attached to communications such as emails and letters.



- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data St Saviour's Ikoyi holds about them (also called 'Subject Access Requests').
- Checking and approving any contracts or agreements with third parties that may handle St Saviour's Ikoyi's sensitive data.

The **ICT department** is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services St Saviour's Ikoyi is considering using to store or process data. For instance, cloud computing services.

### **All staff**

All School staff in whatever role or level within the organisation including Trustees, Board of Management, volunteers, relevant contractors and temporary staff working for the School have the responsibility to abide by this policy.

All staff involved with the collection, processing and disclosure of Personal Data will be aware of their duties and responsibilities by following the guidelines and information will be shared on a need to know basis.

## **18. ENSURING COMPLIANCE**

Training and guidance to comply with the latest data legislation will be provided to all staff. All new staff will be trained on the data protection requirements as part of their induction. Additional group and individual training sessions are provided as required.

## **19. STAFF GUIDELINES**

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers, who in turn must inform the DPO.
- St Saviour's Ikoyi will provide training to all employees to help them understand their responsibilities when handling data.





- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used, and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within St Saviour's Ikoyi or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

## 20. DATA SUBJECT RIGHTS

The GDPR provides the following rights for Data Subjects:

- the right to be informed about the collection and use of their personal data
- the right to access their Personal Data
- the right to have inaccurate Personal Data rectified, or completed if it is incomplete the right to have Personal Data erased
- the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances
- The right to data portability which allows Data Subjects to obtain and reuse their Personal Data for their own purposes across different services. This right only applies to information a Data Subject has provided to the School
- The right to object to the processing of their Personal Data in certain circumstances, for example, for direct marketing
- Rights in relation to automated decision making (making a decision solely by automated means without any human involvement) and profiling (automated processing of Personal Data to evaluate certain things about a Data Subject).

## 21. ACCURACY

The School endeavours to ensure that all Personal Data held is up to date and accurate. Data Subjects should inform the School of any changes to personal details. An individual has the right to request that any incorrect data about them is rectified or corrected.

## 22. RIGHT OF ACCESS

Individuals have the right of access to their personal information, held by the School, within a reasonably practical timescale in line with the latest legislation. The School will verify the identity of the person making the request before any information is supplied.



An individual should make this request in writing to the School.

### 23. RIGHT TO ERASURE

Individuals hold the right to request the deletion or removal of Personal Data where there is no compelling reason for its continued processing.

### 24. DATA BREACH AND COMPLAINTS PROCEDURE

If an individual believes that the School has not complied with this notice or acted otherwise in accordance with the data protection legislation, or believes that a data breach has occurred, they should contact the Administration Manager in writing.

The School will take all steps possible to ensure that it is rectified or corrected. All notifiable breaches will be reported to the relevant supervisory authority within the necessary time frame and guidelines.

### 25. AUDIT AND REVIEW

To ensure compliance with the latest data protection legislation, the School will undertake periodic audits of systems and business processes to identify areas of non-compliance or improvement. This policy will be reviewed periodically and updated in accordance with changes in legislation.

Policy established and agreed:	April 2022
Policy review cycle:	Bi-Annual
Date of next review:	April 2026
Member of staff responsible for the policy	Data Protection Officer, Mrs Ofonagoro