Data protection (GDPR) policy

ICO registration number: Z1782825

Last updated by senior leaders	November 2025
Last reviewed by external data protection officer and internal data protection lead	
Last reviewed by advisory board	
Next review due	September 2026

1 Introduction

1.1 Statutory Guidance

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

- The General Data Protection Regulation (GDPR)
- The Data Protection Act 2018

1.2 Supporting Documents

The following related information is referred to in this policy:

- CCTV Policy
- Safeguarding & Child Protection Policy
- Online Safety Policy

1.3 Terminology

- **Data Subject** means an identifiable 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, a legal guardian, or education guardian.

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

- **School** means St. John's Prep and Senior School.

- **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.

- **Student** or **Students** means any Student or Students in the School at any age.

2 Our commitment to adhering to the UK GDPR and Data Protection Act 2018

- St. John's Prep and Senior School is committed to ensuring the privacy and security of all personal data it holds and processes. In line with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, this policy outlines our approach to handling personal data lawfully, fairly, and transparently.

- This policy applies to all staff, pupils, parents/carers, governors, contractors, and third parties who process personal data on behalf of the school. It aims to ensure that everyone understands their responsibilities in safeguarding personal information and that the rights of individuals are respected and upheld at all times.

- We recognise that effective data protection is critical to maintaining trust and confidence within our school community. As such, we are committed to promoting a culture of data protection awareness and best practice across all aspects of our operations.

3 Statement and Scope of this Policy

- The School collects and processes Personal Data of its Data Subjects and include current, former and prospective Students and their Parents.

- This processing may include obtaining, recording, and 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.

Roles and responsibilities

- To ensure compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, St. John's Prep and Senior School has clearly defined roles and responsibilities for the management of personal data.

The Proprietor

- The Proprietor, who is also the school's Principal, holds overall responsibility for ensuring that the school complies with all relevant data protection obligations. They support a culture of accountability and oversight in relation to data protection.

The Data Protection Officer (DPO)

The school has appointed a Data Protection Officer in line with Article 37 of the UK GDPR. The DPO is responsible for:

- Monitoring the school's compliance with data protection legislation.
- Advising on data protection obligations, including DPIAs.
- Acting as the point of contact for the Information Commissioner's Office (ICO).
- Supporting staff with data protection queries and incident management.
- Overseeing data breach investigations and responses.

- Promoting data protection awareness and training.
- The DPO operates independently and reports directly to the highest level of management. Contact details for the DPO are listed at the end of this policy.

The Data Protection Lead

- The DPL has overall operational responsibility for data protection within the school. They ensure that staff understand their data protection responsibilities and that appropriate resources and training are in place.

The Advisory Board

- The school's advisory board provides external governance, and thus is responsible for regularly checking the school's compliance with data protection legislation, including this policy.

All Staff and Contractors

All staff, supply staff, contractors, governors, volunteers, and others working on behalf of the school are required to:

- Understand and comply with this policy and related procedures.
- Always handle personal data securely and lawfully.
- Report any data protection concerns or breaches without delay.
- Complete mandatory data protection training.
- Seek advice when unsure about handling or sharing personal data.

Failure to follow the school's data protection procedures may result in disciplinary action and, in some cases, legal consequences.

4 Registration as Data Controller

The School is registered as the Data Controller with the Information Commissioner's Office (ICO).

The School's ICO Reference Number **Z1782825.**

This information is provided in accordance with the rights of individuals under:

- Data Protection Act 2018
- General Data Protection Regulations 2018.

5 Purpose

The School collects, stores and processes Personal Data to:

- Carry out its duties and manage its day-to-day operations as a provider of education and as an employer.

- Support Student learning.
- Monitor and report on Student progress.
- Provide appropriate pastoral care.
- Safeguard Students.
- Provide a safe and secure environment.
- Fulfil the School's contractual and legal obligations.

6 Key Principles of GDPR

The School complies with the following principles set out by GDPR.

- **Lawfulness, Fairness, Transparency**: The data held by the school is processed lawfully, fairly and in a transparent manner.

- **Purpose limitation:** All data is collected for specified, explicit, and legitimate purposes and not further processed in a way that is incompatible with those purposes.

- **Data minimisation:** The data held by the school is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

- **Accuracy:** The school ensures that data is accurate and, where necessary, kept up to date; every reasonable step is taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

- **Storage Limitation:** Personal data is not kept for longer than is necessary for the purposes for which it was collected. Once the purpose is fulfilled, the data is deleted or anonymised.

- **Integrity and confidentiality:** The school ensures that we have appropriate security measures in place to protect the personal data held including protection against unauthorised or unlawful processing, accidental loss, destruction, or damage, using appropriate technical and organisational measures.

- **Accountability:** The school is responsible for demonstrating compliance with all the GDPR principles. This includes having appropriate policies, procedures, and documentation in place to show how they are adhering to the regulations.

7 Data Collection

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

8 Personal Data

The School 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 information (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 Privacy Notice

- The School is transparent about the intended processing of data and communicates these intentions via notifications to its Data Subjects prior to the processing of their data.

- The School has published 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.

10 Article 6 Lawful Basis for Processing Data and Article 9 Condition for processing

This section provides information about the legal basis for the school to process Personal Data; the school will determine before processing what is the applicable lawful basis and follow any requirements those lawful bases set out:

- **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 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.

Article 9 of the UK GDPR, special category data—such as information relating to health, ethnicity, religion, or biometric data—requires additional protection due to its sensitive nature. The school only processes special category data where a lawful basis under Article 6 is identified and a specific condition under Article 9 is met. This may include processing necessary for reasons of substantial public interest, such as safeguarding, health and social care, or equal opportunity monitoring, all of which are supported by appropriate policy and safeguards.

11 Handling of Data

- Staff must take care when handling personal data, whether in the classroom, off-site, or working remotely. This includes using password protection, locking screens when unattended, securing physical records, and avoiding the use of unsecured devices or personal email accounts for school data.

- Personal data must not be shared without proper authority and a lawful basis. Any uncertainty about handling or sharing data should be referred to the school's Data Protection Officer.

- Failure to follow data handling procedures may result in disciplinary action and could put individuals and the school at risk of data breaches or legal action.

- Before a new process begins or a new supplier/processor is used, staff will consult with the Data protection officer who will determine if a Data protection Impact Assessment is required. Failure to do so will result in disciplinary and potential fines from the ICO.

11.1 Authorised disclosures of Personal Data to third parties:

Any information which falls under Personal Data will only be disclosed to third parties where there is a lawful basis under the UK GDPR and it is necessary and proportionate to do so. This includes, but is not limited to:

- Compliance with a legal obligation (e.g. to the Department for Education, local authority, HMRC, or law enforcement agencies)
- Where necessary for the performance of a contract (e.g. with service providers such as IT support or catering contractors)
- Where explicit consent has been given by the data subject
- To safeguard pupils or individuals (e.g. health and social care services, safeguarding authorities)

- Where the disclosure is otherwise permitted under data protection legislation.

All third parties receiving personal data must have appropriate technical and organisational measures in place to protect the data, and where required, data sharing or processing agreements will be in place to ensure ongoing compliance with UK GDPR standards.

12 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. An exemption applies when disclosing as part of a Subject Access Request (SAR).

- 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.

13 Data Transfer

The school does not routinely transfer personal data outside of the United Kingdom. However, in circumstances where such transfers are necessary — for example, when using certain cloud-based educational platforms or services hosted overseas — the school ensures that appropriate safeguards are in place to comply with the UK General Data Protection Regulation (UK GDPR).

Any transfer of personal data to a country outside the UK will only take place where the UK Government has determined that the destination offers an adequate level of data protection, or where alternative legally recognised safeguards are in place. These safeguards may include the use of Standard Contractual Clauses, an International Data Transfer Agreement, or other mechanisms approved by the Information Commissioner's Office.

Before any international transfer is made, the school will assess the risks and, where necessary, complete a Data Protection Impact Assessment. All transfers will follow the principle of data minimisation, ensuring that only the necessary data is shared and that it is handled securely.

14 Data Retention and Record Keeping

The School has a duty to retain Personal Data for a period for legal and other legitimate reasons. Some data is retained following both staff and pupils' departure from the School. The School's guidance on data retention defines the length of time for which Personal Data and records are kept.

14.1 Retention of Personnel Records

- Colleagues' personnel records and successful candidates' data are stored securely.

- Colleagues' personnel records are retained for 6 years after the employee has left St. John's Preparatory and Senior School. All digital data are securely and permanently deleted.

- Where there has been a CP/safeguarding allegation made against a colleague, the School retains their personnel records for 10 years or until the employee reaches retirement age, whichever is the longer.

- Colleagues' email accounts are securely retained for three months (or six months for senior leaders, aside from the DSL whose email account is retained for one year) after their departure, *unless involved in a safeguarding allegation that led to police action in which case they are kept indefinitely*.

- Any records that could be called as evidence in legal proceedings e.g. records relating to child sexual abuse concerns/disclosures or allegations against colleagues are kept indefinitely as advised by the police and/or legal counsel.

- To provide feedback and resolve potential queries, we save unsuccessful candidates' personal data for up to six months following the end of the selection process.

14.2 Retention of Pupil Records

- Where a pupil comes off our roll before the conclusion of Year 13, their records (including CP/safeguarding files) are forwarded securely to their new school/college.

- Pupils' school email accounts are deleted when they come off our roll.

- Where a pupil is on roll with St. John's at the conclusion of the final academic year offered (Year 13), the school takes responsibility for the secure retention and storage of their records, including CP/safeguarding files.

- Where a pupil is on roll with St. John's at the conclusion of the final academic year offered and the pupil was never a 'looked after child', their records will be retained by St. John's School for 10 years, or until the conclusion of the academic year in which the pupil's year group reach their 25th birthday. Specifically, their CP/safeguarding files containing documentation relating to any referrals to social care services or any other social care services involvement will be kept until 35 years from date the pupil leaves the school.

- Where a pupil is on roll with St. John's at the conclusion of the final academic year offered (Year 13) and the pupil was at any point a 'looked after child', all records (including CP/safeguarding files) will be retained until the pupil's 75th birthday.

15 Data Protection contacts

Data Protection Lead

- The GDPR Lead, Mr. D. Brandon, has overall operational responsibility for data protection within the School. Any contact relating to the School's handling of data should be directed to him via gdpr@stjohnsprepandsenior.co.uk

Data Protection Officer

- The Data Protection Officer has the delegated responsibility for overseeing this policy and ensuring compliance with all relevant data protection legislation and is responsible for ensuring that processes are in place to safeguard the integrity of the school's data.

  GDPR in Schools
  11 Kingsley Lodge
  13 New Cavendish Street
  London W1G 9UG

16 Ensuring Compliance

Training and guidance to comply with the latest data legislation is provided to all staff. All new staff are trained on data protection requirements as part of their induction.

Additional group and individual training sessions are provided as required.

17 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
  - Individuals have the right to be told how their data is collected, used, stored, and shared, typically through a privacy notice.
- The right to access their Personal Data

    - Individuals can request a copy of the personal data the school holds about them.
- The right to rectification
    - Individuals have the right to request that inaccurate or incomplete personal data is corrected without delay.
- The right to have Personal Data erased.
    - In certain circumstances, individuals can ask for their personal data to be deleted.
- The right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances
    - Individuals can request that the school limits how their data is used, particularly if accuracy is contested or processing is unlawful.
- The right to data portability
    - In specific situations, individuals can request their data be transferred to another organisation in a structured, commonly used format.
- The right to object to the processing of their Personal Data
    - Individuals can object to the processing of their data in certain cases, such as for direct marketing or where processing is based on legitimate interests.
- Rights in relation to automated decision making and profiling.
    - Individuals have the right not to be subject to a decision based solely on automated processing, including profiling, unless specific conditions are met.

18 Subject Access Requests (SARs) and other requests for data.

All individuals have the right under the UK General Data Protection Regulation to request access to the personal data the school holds about them. These are known as Subject Access Requests (SARs). In addition, individuals may exercise other data protection rights, such as the right to rectification, erasure, restriction, or objection to processing.

If a SAR or any other request related to personal data is received by a member of staff—whether in writing, verbally, via email, or through a parent, carer, or pupil—it must be immediately referred to the school's Data Protection Lead (DPL). Staff must not attempt to respond to the request themselves.

The DPO is responsible for:

- Acknowledging and recording the request.
- Verifying the identity of the requester where necessary.
- Assessing the scope and nature of the request.
- Coordinating the collection, review, and disclosure of relevant data.
- Ensuring that the response is issued within the statutory timeframe of one calendar month, unless an extension is justified under the UK GDPR.

Delays in passing on requests can impact the school's ability to meet legal deadlines. It is therefore essential that all staff are vigilant and understand the importance of forwarding any such requests to the DPO without delay.

Fees may be applied if the request is deemed manifestly unfounded and/or excessive. In such cases, St. John's reserves the right to ask the requester to reconsider or charge a proportionate administration fee.

19 Data Breach and Complaints Procedure

Under the UK General Data Protection Regulation (UK GDPR), a personal data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. Breaches can occur through both human error and malicious activity, and may affect digital or paper records.

All staff and contractors have a duty to report any suspected or confirmed data breach immediately to the school's Data Protection Officer (DPO). This includes incidents such as:

- Loss or theft of devices or paper files containing personal data
- Emails or letters sent to the wrong recipient
- Unauthorised access to personal information
- Accidental deletion or alteration of records
- Cybersecurity incidents (e.g. malware, phishing attacks)

Staff must not try to investigate or contain the breach themselves. Prompt reporting is essential to allow the DPL to assess the severity of the incident, take appropriate containment steps, and determine whether the breach needs to be reported to the Information Commissioner's Office (ICO).

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the DPL will ensure it is reported to the ICO within 72 hours of the school becoming aware of it. Affected individuals may also need to be informed if the breach poses a high risk to their rights.

A central record of all personal data breaches is maintained by the DPL, regardless of whether they are notifiable to the ICO.

Failure to report a breach appropriately may result in disciplinary action and put the school at risk of regulatory penalties. All staff must therefore remain vigilant and understand their role in safeguarding personal data.

The school uses the GDPRiS platform (accessible at app.gdpr.school) to manage data protection compliance. In the event of a suspected or confirmed data breach,

staff are required to promptly log into the platform and submit the details using the Incident and Breach Reporting Tool.

Submitting the breach through GDPRiS will automatically notify the Data Protection Officer, who will assess the incident and take appropriate action in line with the school's data breach response procedures. Timely reporting is essential to ensure that the school can fulfil its legal obligations, including any requirement to notify the Information Commissioner's Office within the statutory timeframe.

If you do not have access to the platform, you must email the in-school Data Protection Lead as identified in this policy, so the breach can be recorded and escalated without delay.

20 Audit and Review

To ensure compliance with the latest data protection legislation, the School undertakes periodic audits of systems and business processes to identify areas of non-compliance or improvement.

This policy is reviewed at least annually and updated in accordance with changes in legislation.

SUBJECT ACCESS REQUEST FORM

Please complete the following form and return it to the school office.

Data Subject Details

Title	
Surname	
First Name(s)	
Current Address	
Telephone	
Email address	
Date of birth	
Details of identification provided to confirm name of data subject in question	
Details of Subject request	

If the person requesting the information is NOT the data subject, complete the below:

Are you acting on behalf of the data subject with their written consent or in another legal authority?	Yes No
If 'Yes' please state your relationship with the data subject (e.g. parent, legal guardian, or solicitor)	
Has proof been provided to confirm you are legally authorised to obtain the information? (e.g. letter of authority)	Yes No

If you are a parent, please provide proof of parental responsibility. Personal data of a child cannot be released without it.

3rd Party Requestor Details

Title	
Surname	
First Name(s)	
Current Address	
Telephone	
Email address	

Declaration

I hereby request that St. John's Prep and Senior School agree to proving me the specified information requested about the data subject above.

Name	
Signature	
Date	