St George's
PREPARATORY SCHOOL
Preparing Children For Life

Author – I. Watson

Agreed by Directors and Available to Staff– January 2021	
To be Reviewed – Annually	**Last Review Date:** May 2022

Data Protection Policy

Contents:

Appendices:

- **Data Disposal Schedule (Appendix 1)**
- **Data Breach Procedure Checklist (Appendix 2)**
- **GDPR Issues Log (Summary) Template (Appendix 3)**
- **Employee Code of Practice for Handling Personal Information**

Introduction:

Handling & processing of data in any organization needs to be approached methodically, thoroughly and consistently with due regard to current legislation governing its gathering, generation, storage, processing, availability and disposal.

The processing of personal data is essential to the operation of the school and consists of five main streams: Pupils, Parents, Governors, Employees and Alumni.

In order to be lawful, personal data can only be processed:

- With the consent of the individual
- It is necessary for contractual reasons
- It is required under a legal obligation, by statute or Court Order
- It is necessary in order to pursue the legitimate interests of the data controller
- If someone acting on the data subject's behalf has their written consent
- To enable prevention or detection of a crime
- For obtaining legal advice
- For preventing damage to health

In order to be lawful, sensitive personal data can only be processed:

- With explicit informed consent (eg letter from parent)
- To satisfy employment obligations (eg HR administration)
- In the vital interests of the data subject or another person (eg medical emergency)
- The information has already been made public (deliberately) by the data subject
- In relation to legal proceedings or advice
- In relation to specific Public functions / services (eg tax or social security issues)
- For medical purposes

It is fundamentally important that appropriate procedures and governance are in place to protect the confidentiality and use of this data as well as the reputation, integrity and trust of the School.

Purpose of the Policy:

This policy is intended to provide a straight forward, transparent and auditable process to enable routine contact with parents and to ensure the education, safety and welfare of the children within the school. It also provides a high-level overview of procedures designed to ensure consistent understanding and practice by all employees and the school's data processing parameters relating to:

- Privacy
- Data Collection
- Data Retention
- Data Storage
- Data Sharing
- Data Disposal
- CCTV Policy
- Taking, Storing and Using Images of Children
- Training Procedures
- Actions in the event of an internal or external breach

Privacy Statement:

- The Bursar is the designated Data Protection Officer (DPO) for St George's Preparatory School.
- Relationships with all potential 'third party' data handlers (including ICT & Systems Support Services, other schools, the Education Department, photographers, media requests) are managed through the Bursar's Office.
- St George's Preparatory School do not capture or store any personal information about you when you access our website unless you voluntarily elect to give us that information by email, using an electronic form or enquiring about our services.
- When you do provide us with your personal information, it will be stored and used for the specific purpose intended. We will not share the information you provide with any third party without specific permission in accordance with the Data Protection (Jersey) Law 2018.
- Some areas of our website offer e-mail updates and we also offer access to our Parent's Portal. To receive updates, you are required to register by providing your e-mail address, a user name and password. We will not share the information you provide with any third party in accordance with the Data Protection (Jersey) Law 2018.
- Links that may appear on our web site from time to time leading to other web sites does not mean that third parties can access any personal information held by St George's Preparatory School. However, our Privacy Statement covers only the stgeorgesprep.co.uk website and we are not responsible for the content of any external websites so always check the privacy Statement on any site that you access.
- A computer's IP address is a number assigned for use of the internet. Although an IP address is recorded in a log file when you visit our website, this does not contain any personal identifiable information about the individual user.

- St George's Preparatory School comply with the Data protection (Jersey) Law 2018 and base our procedures for handling personal data on guidelines within that act. Personal information collected and held will not be disclosed to any third party without the individual's prior consent or the requestor's demonstrated legal authority to receive it.
- St George's Preparatory School retain the right to revise this Privacy Statement without notice but will do so only in line with changes to our holistic GDPR Policy. Continued use of the stgeorgesprep.co.uk website after a change is deemed as individual acceptance of the change.

Principles & Purposes of Processing:

- Parental Responsibility (PR) should be established and recorded by the school to ensure that only those with PR can access personal information regarding the child. Responses to access requests will be based on proof of identity and the information currently held by the school. It is imperative therefore that any changes to personal circumstances must be notified to the school and to the DPO immediately.
- All interactions and internal processes will reflect the principles set out in this Policy and be applied for specific circumstances e.g. admissions, school visits, photography etc.

Data Collection:

- All data must be relevant, accurate and not excessive. It is collected for a specific purpose and is not shared with any third parties for supplementary or commercial purposes.

Data Retention:

- All personal data collected will be held securely for the minimum period necessary to complete its specific purpose.
- Legally binding retention periods relating to various types of data processed is attached as Appendix 1.

Data Storage:

- All electronic data stored at St George's Prep can only be accessed by employees via a PC using personal user name and password.
- Internal control of access permissions to drives & network files are reviewed annually by the Bursar or Assistant Bursar to ensure permissions are still valid.
- All PCs or electronic devices where personal data is stored must be locked at all times when not in use (on or off site) and closed down at the end of each day to prevent unauthorised access to this data by unauthorized third parties. Particular care is to be taken when accessing the network remotely.
- All employee passwords are unique to the user name and no access log ins are to be shared.
- Incoming and outgoing e-mail communications are monitored periodically by the Bursar or Assistant Bursar to ensure appropriate usage or to identify potential compliance issues.
- Hard copy documents and archive materials are stored in locked units and secure locations.

Data Sharing:

- No personal information will be disclosed to any unauthorized third party without the individual's prior consent or the requestor's demonstrated legal authority to receive it.
- Where electronic operating systems are in use, all data is held and processed securely in line with GDPR legislation.

Data Access:

- Different data sets may need to be seen by different members of staff. No personal or pupil information is to be shared between data holders or with other staff within the school unless there is a specific involvement with that individual or process.
- No personal information or information relating to the school's business is to be shared with any internal / external third parties at any time on or off the school premises.
- Any individual employee or parent / guardian (with Parental Responsibility (PR) for their child) has the right to request access to / sight of any information held about them by St. George's Preparatory School.
- Access to an individual's own data should be requested in writing to the Bursar (48 hours notice required).

Data Disposal:

- All electronic data is archived or deleted depending on requirements stated in the retention policy outlined in Appendix 1.
- If PCs or other electronic devices are no longer operational, all hard drives are removed and destroyed in a secure environment prior to disposal of the device.
- All confidential hard copy data is archived or shredded (either internally or through a contracted third party processor) depending on the requirements stated in Appendix 1.

Key Requirements & Controls:

- Data Protection Impact Assessments to be completed for all key data handling processes in line with the school's Risk Management Strategy.
- A GDPR Risk Register is maintained by the Bursar to record all incidents or data Protection breaches and how these have been resolved. All breaches must therefore be reported in writing to the Bursar within 24 hours of the incident.
- Monthly audit checks of specific data handling processes will be undertaken by the Internal Auditors and recorded on a checklist. Remedial actions & time scales will also be recorded & reported to the Information Committee & Board of Directors.

Training:

- Specific GDPR Training logs set up for Data Handlers and all staff.
- Training will include: GDPR policy & Employee Code of Practice sign off; Roles & responsibilities (data handling processes in the employee's specific work area); DPIAs; Record keeping; definition of a breach; Reporting procedures; Access Request Procedures

- Data Protection training is included in the revised Induction Process for new employees.
- Updates to Policy to be advised to all data handlers by the DPO as they are implemented.
- Refresher training to take place at regular intervals to ensure knowledge & skills base retained.

CCTV Policy:

- CCTV is operational within the school buildings and grounds for safeguarding and security purposes only. Appropriate signage is displayed.
- CCTV Footage is retained for 30 days as a minimum legal requirement and then over-written.
- CCTV can only be accessed by the Bursar, Headmaster (or their deputies) or the Property & Maintenance Manager to view footage should any incident be reported.
- CCTV footage may be retained for use in any school security, safeguarding or GDPR related investigation. No footage will be retained for any other reason or shared with provided to unauthorized third parties at any time.

Visitor Management System (VMS):

- From September 2019, a new GDPR compliant Visitor Management System will be in use at St George's Preparatory School. All visitors will be required to log in (if not already preregistered) and provided with a badge which must be permanently displayed while on site.
- The same system will be used to record late arrival of pupils or those being taken out for / returned to school after appointments. This process requires a photographic image of the responsible parent / guardian removing the child from school to be recorded for safeguarding purposes. This information will be stored securely but cleared within one calendar month.
- Staff ID cards will also be recorded on the system to identify who is on or off site at any given time in line with the School's Health & Safety Policy.

Taking, Storing & Using Images of Children:

- Images of children will not be taken for use in publicity materials produced by the school or for use by any external media organisations without parental consent. This consent extends to the use of the child's first name only, the Image only and to the use of first name and image.

What constitutes a breach of the Data Protection Policy?

- Any loss, theft or misplacement of personal or sensitive data whether by accident or malicious intent constitutes a potential breach of data protection and must be reported to the Bursar / DPO in writing within 24 hours of the incident.

Actions in the Event of an Internal or External Breach:

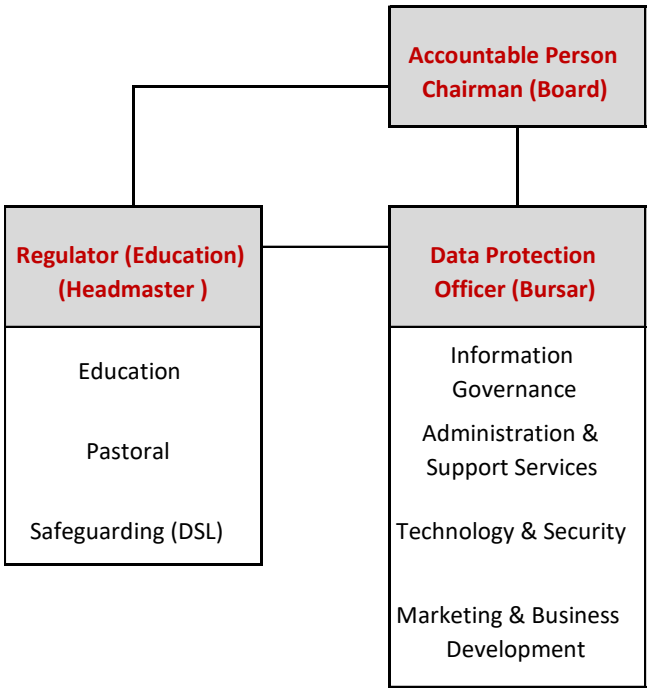
- Any incident or potential breach of GDPR Regulations will initially be recorded in an Incident Log stating the date, time and nature of the reported breach. The Log will act as a summary and be updated to include resolution and actions taken to prevent any re-occurrence.
- A more detailed Data Breach Procedure Checklist will also be completed to define the perceived impact of the breach, the investigation process & the most appropriate response.

- All significant breaches are reported to the Office of the Information Commissioner within 72 hours.

Key Internal Roles & Responsibilities:

- It is the responsibility / duty of all staff to report any potential breach of the School's Data Protection Policy to the Bursar / DPO in writing within 24 hours of the incident (even if they are responsible for the breach). Written notification provides the start of the process audit trail and is therefore crucial to the efficient handling of the situation.
- The key individual in ensuring compliance with this Policy on a day to day basis is the Bursar / DPO. The initial point of contact for most data received by the school for processing is through 'Data Handlers' in the Bursar's Office and Administration Team. The Bursar also acts as the Internal Auditor in respect of all non-educational data processing.
- The Internal Auditor for educational, pastoral & safeguarding data is the Headmaster.
- The Information Governance Committee (Chairman, Headmaster and Bursar) shall meet once per term prior to the Director's Board Meeting to enable current information to be circulated.

St George's Preparatory School - GDPR Organisation Chart:



Specific Roles & Responsibilities:

- The following table outlines the specific data handling responsibilities for the day to day operation at St George's Preparatory School.

- It defines these responsibilities in terms of day to day processing tasks including collection, retention, storage and disposal of data.
- The table also identifies the Senior Management responsibility for monitoring, auditing and reporting on these processes.

Nature of Data	Data Handler	Regulator /Auditor
Admissions, Progress & Leavers	School Secretary	Bursar
Medical Data	School Secretary	Bursar
Marketing & Communications	Marketing & Business Development Officer	Bursar
Development & Alumni	Marketing & Business Development Officer	Bursar
Education	Class, Form or Specialist Teacher	Headmaster
Pastoral Information	Form Teacher or Deputy Head (Pastoral)	Headmaster
Disciplinary Information (Pupils)	Form Teacher or Deputy Head	Headmaster / Bursar
Incidents & Accidents	First Aid Staff, Form Teachers, Sports Staff	Bursar
Safeguarding	Designated Safeguarding Lead (DSL)	Headmaster
Recruitment (Employee)	Admin Assistant, Interview Panel	Bursar
Disciplinary Information (Employee)	Headmaster & Bursar	Chairman (Board)