Vita et Pax
PREPARATORY SCHOOL

Vita et Pax Preparatory School
Established 1936

Data Protection Policy

Policy Originator	Head Teacher
Approved by	Governing Body
Date Approved	1 March 2026
Status	Statutory
Review Period	Annually (next: March 2027)
Data Controller	Vita et Pax Preparatory School
Data Protection Lead	Jevash Dey (Business Manager)
Data Protection Co-ordinator	Maria Castro

1. Introduction

Vita et Pax Preparatory School collects, stores and processes personal data about staff, pupils, parents, governors, contractors and other third parties in the course of its activities. The school is the data controller and is legally responsible for ensuring that all personal data is handled in compliance with data protection law.

This policy is informed by:

- The UK General Data Protection Regulation (UK GDPR).
- The Data Protection Act 2018 (DPA 2018).
- Keeping Children Safe in Education (KCSIE) 2025.
- The Freedom of Information Act 2000 (as applicable).
- The Privacy and Electronic Communications Regulations 2003.
- ICO guidance for schools and education providers.
- The Independent School Standards Regulations (ISSRs) 2014.

2. Scope

This policy applies to all members of the school community who handle personal data, including employees, governors, contractors, volunteers and any other person processing data on the school's

behalf. Breaches of this policy by staff may result in disciplinary action. Contractors are bound by data processing agreements.

3. Key Definitions

- Data controller — the school, which determines the purposes and means of processing.
- Data processor — an organisation that processes data on the school's behalf (e.g., payroll provider, IT suppliers, NeuralShield).
- Personal data — any information relating to an identifiable living individual, including names, ID numbers, contact details, photographs and online identifiers.
- Special category data — data revealing racial/ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life/orientation, genetic or biometric data. Criminal conviction data is treated equivalently.
- Processing — any operation on personal data: collection, storage, analysis, sharing, alteration, deletion or destruction.
- Personal data breach — a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. Data Protection Responsibilities

- The Governing Body / Proprietorial Body has overall accountability for data protection compliance and ensures adequate resources and training are in place.
- Data Protection Lead — Jevash Dey (Business Manager) is responsible for ensuring day-to-day compliance, maintaining records of processing activities, advising staff on data protection matters, and liaising with the ICO where necessary.
- Data Protection Co-ordinator — Maria Castro supports the DPL with operational data handling, subject access requests and breach reporting.
- The Head Teacher (Darren May) ensures this policy is implemented and that staff understand their responsibilities.
- The DSL (Darren May) ensures that data protection considerations are balanced appropriately with safeguarding duties — data protection law does not prevent sharing information for safeguarding purposes.
- All staff must handle personal data fairly, lawfully, responsibly and securely. Staff must attend data protection training and report any breaches immediately.

5. The GDPR Principles

The UK GDPR sets out six principles which govern all processing of personal data. The school must comply with all six:

1. Lawfulness, fairness and transparency — personal data must be processed lawfully, fairly and in a transparent manner. Individuals are informed through Privacy Notices.
2. Purpose limitation — data is collected for specified, explicit and legitimate purposes and not processed in a manner incompatible with those purposes.
3. Data minimisation — data collected is adequate, relevant and limited to what is necessary for the purpose.

4. Accuracy — personal data is kept accurate and up to date. Inaccurate data is corrected or erased without delay.

5. Storage limitation — data is kept for no longer than necessary. The school's Retention of Records schedule sets out specific retention periods.

6. Integrity and confidentiality (security) — appropriate technical and organisational measures ensure security of personal data.

The broader accountability principle requires the school to demonstrate compliance through records, policies, training logs, impact assessments and audit trails.

6. Lawful Bases for Processing

The school relies on one or more of the following lawful bases for processing personal data:

- Consent — the individual has given clear, informed consent. Used sparingly; can be withdrawn at any time.
- Contract — processing is necessary for a contract with the individual (e.g., employment contracts, parent-school agreements).
- Legal obligation — processing is necessary to comply with the law (e.g., safeguarding, tax, health and safety, KCSIE).
- Vital interests — processing is necessary to protect someone's life (e.g., medical emergencies).
- Public task — processing is necessary for the school's educational function.
- Legitimate interests — processing is necessary for the school's legitimate interests (e.g., security, IT monitoring via NeuralShield), balanced against the individual's rights.

For special category data, additional conditions apply, including explicit consent, safeguarding obligations, employment law, vital interests, and substantial public interest (e.g., preventing unlawful acts, protecting children).

7. Privacy Notices

The school publishes Privacy Notices to inform individuals about how their data is processed. Separate notices are maintained for:

- Staff — the Staff Privacy Notice.
- Parents and pupils — the Privacy Notice and Data Protection Policy (on the school website).
- Visitors and contractors — provided at sign-in.
- Job applicants — provided during the recruitment process.

Privacy Notices include: the identity of the data controller, the purpose and lawful basis for processing, who data is shared with, retention periods, and the individual's rights.

8. IT Monitoring, NeuralShield and CCTV

The school operates the following monitoring systems as part of its safeguarding and security obligations:

- NeuralShield — an AI-powered network safeguarding system that monitors and filters all internet traffic on the school network. NeuralShield processes DNS queries, browsing metadata and network activity data. This processing is necessary for the school's legitimate interests in

safeguarding and security, and to comply with KCSIE 2025 requirements for filtering and monitoring. Monitoring data is accessible only to the IT Lead and DSL.

• CCTV — security cameras operate on the school premises for safety and security purposes. Footage is retained for a maximum of 30 days unless required for an investigation. CCTV is operated in accordance with the ICO's Code of Practice.

• Email and IT systems — the school monitors use of school email and IT systems in accordance with the IT Acceptable Use Policy and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

All monitoring is proportionate, conducted for defined purposes, and disclosed to individuals through the relevant Privacy Notices.

9. Data Security

The school takes appropriate technical and organisational measures to protect personal data against unauthorised access, loss, destruction or damage:

• Access to personal data is restricted by role-based permissions.

• School systems are protected by passwords, and MFA where available.

• Portable devices and removable media containing personal data must be encrypted.

• Personal data must not be removed from school premises without prior authorisation from the Data Protection Lead.

• Personal email accounts must not be used for school business.

• Paper records containing personal data are stored in locked cabinets and disposed of securely (cross-cut shredding).

• NeuralShield provides network-level security monitoring, intrusion detection and malware blocking.

• Staff receive data security training at induction and through annual refreshers.

10. Data Breach Reporting

All personal data breaches — suspected or confirmed — must be reported immediately to the Data Protection Lead (Jevash Dey) or Data Protection Co-ordinator (Maria Castro). Examples of breaches include:

• Loss of an unencrypted device, USB stick or physical file containing personal data.

• Hacking, malware or ransomware affecting school systems.

• Misdirected email, post or fax containing personal data.

• Failure to BCC recipients of a mass email.

• Unsecure disposal of records containing personal data.

• Unauthorised access to personal data by staff or third parties.

The school will assess each breach and, where it poses a risk to individuals, report it to the ICO within 72 hours. Where the breach poses a high risk to individuals' rights and freedoms, the affected individuals will also be notified. All breaches are logged, regardless of whether they are reported to the ICO.

Falling victim to a data breach (e.g., by human error) will not always be a disciplinary matter. However, failure to report a breach is a serious disciplinary offence.

11. Rights of Individuals

Individuals have the following rights under the UK GDPR. Any request to exercise these rights must be reported immediately to the Data Protection Lead:

- Right of access (Subject Access Request): the right to obtain a copy of personal data held about them. The school must respond within one month.
- Right to rectification: the right to have inaccurate data corrected.
- Right to erasure: the right to have data deleted in certain circumstances (this is not absolute — safeguarding and legal obligations may override it).
- Right to restriction: the right to restrict processing in certain circumstances.
- Right to data portability: the right to receive data in a structured, commonly used format.
- Right to object: the right to object to processing based on legitimate interests.
- Right to withdraw consent: where consent is the lawful basis.
- Right relating to automated decision-making: the right not to be subject to decisions based solely on automated processing (including profiling) that produce legal or significant effects.

These rights are not absolute and exceptions may apply. The school will respond to requests within one month (extendable by two months for complex requests).

12. Safeguarding and Data Sharing

Data protection law does not prevent the sharing of information for safeguarding purposes. KCSIE 2025 is clear: fears about sharing information must not be allowed to stand in the way of the need to promote the welfare and protect the safety of children. Staff should not assume that someone else will share relevant information. If in doubt, consult the DSL.

13. Data Retention

Personal data is retained only for as long as necessary. Key retention periods:

Data Category	Retention Period
Staff personnel records	6 years after leaving
Unsuccessful applicants	6 months after recruitment decision
Pupil records	Until pupil's 25th birthday
Safeguarding/child protection records	Until pupil's 25th birthday (or longer if required)
Low-level concerns	At least 7 years post-termination
Accident/incident records	At least 3 years (or age 25 for minors)
CCTV footage	30 days (unless needed for investigation)
NeuralShield monitoring logs	Per data retention schedule
Financial records	7 years (HMRC requirements)
DBS certificates	6 months after receipt (number retained on SCR)

Data Category	Retention Period
Governors' records	6 years after term ends

14. Data Protection Impact Assessments (DPIAs)

A DPIA is carried out before any new processing activity that is likely to result in a high risk to individuals' rights and freedoms. This includes new IT systems, CCTV changes, or new data-sharing arrangements. DPIAs are conducted by the Data Protection Lead and reviewed by the Head Teacher. A record of all DPIAs is maintained.

15. Financial and Payment Card Data

The school complies with the Payment Card Industry Data Security Standard (PCI DSS). Staff who process payment card data must follow PCI DSS requirements. Financial information (bank details, salary, NI numbers) must be handled with the same care as legally sensitive data, given its potential for harm if compromised.

16. Training

All staff receive data protection training at induction and through annual refresher sessions. Training covers the GDPR principles, breach reporting, subject access requests, secure data handling and the relationship between data protection and safeguarding. Governors receive data protection awareness training. Training records are maintained by the Data Protection Lead.

17. Related Policies

- Staff Privacy Notice
- Privacy Notice for Parents and Pupils
- IT Acceptable Use Policy
- Child Protection & Safeguarding Policy
- Low-Level Concerns Policy
- Retention of Records Schedule
- Complaints Policy

18. Contact and Complaints

- Data Protection Lead: Jevash Dey — j.dey@vitaetpax.co.uk
- Data Protection Co-ordinator: Maria Castro — m.castro@vitaetpax.co.uk
- Head Teacher: Darren May — head@vitaetpax.co.uk
- School Office: 020 8449 8336

- ICO: www.ico.org.uk — 0303 123 1113

Approved by: Governing Body of Vita et Pax Preparatory School

Date: 1 March 2026