Data Protection (GDPR) Policy

Approved by the Headteacher and Governing Body on 13.10.25

Reviewed: 09.25
To be reviewed: 09.26

Policy Area	GDPR
Reviewed by	Mr David Swanston (DSL) & Mr Steve Irvine (Online Safety Lead)
Approved by	Governing Body – Mrs Bernadette Buckle (Safeguarding Governor)
SLT Oversight	Mr Lee Green
Review Date	September 2025
Next Review Due	September 2026

Summary of Key Points (2025 Revision)

- Aligns with UK GDPR (2024 update) and Data Protection Act 2018.
- Complies with *DfE Cybersecurity Standards for Schools (2023)*.
- Clarifies roles of Data Protection Officer (DPO), DSL, and Network Manager.
- Integrates guidance from *Information Commissioner's Office (ICO)*.
- Strengthens procedures for subject access requests (SARs).
- Adds sections on data breach reporting and cybersecurity standards.
- Embeds accessibility and inclusive data handling for SEND learners.

1 Purpose and Scope

This policy sets out how St Vincent's School complies with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.
It applies to all staff, governors, volunteers, contractors, and third parties who process personal data on behalf of the school.

2 Legislative Framework

- UK GDPR (2024 update)
- Data Protection Act 2018
- Education (Information About Individual Pupils) Regulations 2013
- Freedom of Information Act 2000
- DfE Cybersecurity Standards for Schools (2023)
- Keeping Children Safe in Education (2025)

3 Definitions

Personal data: information relating to an identified or identifiable individual.
Special category data: information revealing racial origin, religious beliefs, health or disability data.
Processing: any operation performed on data (e.g., collecting, storing, sharing).
Data subject: the individual whose data is processed.
Data controller: the organisation that determines why and how personal data is processed.
Data processor: any third party acting on behalf of the controller.

4 Roles and Responsibilities

- Data Controller: St Vincent's School Governing Body.
- Data Protection Officer (DPO): [Insert appointed DPO name / service provider].
- Senior Information Risk Owner (SIRO): Mr Lee Green.
- Designated Safeguarding Lead (DSL): Mr David Swanston.
- ICT / Network Manager: Mr Steve Irvine (Online Safety Lead).
- All Staff: must handle data lawfully and complete annual GDPR training.

5 Data Protection Principles

St Vincent's School adheres to the seven UK GDPR principles:

1. Lawfulness, fairness and transparency – processed with a clear legal basis.
2. Purpose limitation – used only for specified purposes.
3. Data minimisation – limited to what is necessary.
4. Accuracy – kept up to date.
5. Storage limitation – retained only as long as necessary.
6. Integrity and confidentiality – protected by technical and organisational measures.
7. Accountability – school demonstrates compliance through records and audits.

6 Lawful Bases for Processing

Processing is lawful under UK GDPR where it is necessary for:

- Performing a public task in the public interest (education provision).
- Compliance with legal obligations (e.g., DfE returns).
- Protecting vital interests of pupils or staff.
- Contractual requirements (employment contracts, service agreements).
- Consent (for optional activities, photography, website use).

Special category data is processed under Article 9(2)(g) and Schedule 1 of the Data Protection Act 2018 (substantial public interest).

7 Collecting and Using Personal Data

- Data is collected from parents, pupils, staff and agencies only for legitimate educational purposes.
- Data is processed securely using approved systems (e.g., MIS, CPOMS, RM SafetyNet monitoring logs).
- Only authorised staff have access to sensitive information.
- Privacy notices are published on the school website.

8 Data Sharing

- Shared only where legally permitted and necessary (for example with DfE, LA, Ofsted or NHS services).
- Third-party processors must sign a Data Processing Agreement and demonstrate GDPR compliance.

- No data is transferred outside the UK without appropriate safeguards.

9 Data Retention and Disposal

- The school follows the *Information and Records Management Society (IRMS) School Toolkit*.
- Retention periods are defined for each record type.
- Secure disposal via confidential shredding or certified digital deletion.

10 Subject Access Requests (SARs)

- Requests must be submitted in writing to the DPO.
- Identity is verified before data is released.
- Response provided within one month (extendable for complex requests).
- Information may be withheld only where permitted by law (e.g., third-party data protection).

11 Data Breach Management

- All suspected breaches reported immediately to the DPO and SIRO.
- Logged and investigated within 24 hours.
- ICO notified within 72 hours if the breach poses risk to individuals.
- Affected data subjects informed without undue delay.
- Lessons learned are used to improve controls.

12 ICT and Cybersecurity Controls

- Network protected by firewalls, endpoint protection and RM SafetyNet filtering.
- Multi-factor authentication used for remote systems.
- Regular patching and back-ups.
- Annual penetration testing and risk assessments undertaken.

13 Data Protection Impact Assessments (DPIAs)

DPIAs are carried out for any high-risk processing (e.g., new systems, CCTV, biometrics). Templates and guidance follow ICO standards.

14 Training and Awareness

- All staff receive GDPR induction and annual refresher training.
- Governors receive oversight training to understand their responsibilities.
- Data protection guidance is displayed in staff rooms and shared drives.

15 Complaints

Data-protection concerns should first be raised with the DPO.
If unresolved, complaints may be escalated to the Information Commissioner's Office (ICO):
ICO Helpline 0303 123 1113 | www.ico.org.uk

16 Monitoring and Review

- The DPO and SIRO monitor compliance through audits and spot checks.
- The policy is reviewed annually or following legislative changes.
- Approval is recorded in governing-body minutes.

Appendix A - St Vincent's School – Record of Processing Activities (ROPA)

(Compliant with Article 30, UK GDPR – reviewed September 2025)

Category of Data Subject	Type of Personal Data Processed	Purpose of Processing	Lawful Basis (Article 6)	Special Category Data (Article 9)	Data Sharing / Recipients	Retention Period	Security Measures
Pupils	Name, address, DOB, gender, UPN, medical info, SEN/EHCP data, attendance, progress, behaviour, safeguarding records	Delivering education, safeguarding, tracking progress	Public Task / Legal Obligation	Health data, SEND needs, ethnicity	DfE, LA, NHS, social care, parents	Until pupil reaches age 25 (Safeguarding/education records)	Encrypted MIS (e.g. SIMS/Arbor), password-protected files
Parents / Carers	Name, contact details, relationship to pupil, correspondence records	Communication and emergency contact	Public Task / Legal Obligation	N/A	Staff, DSL, emergency services (where necessary)	One year after pupil leaves	Restricted access; school email only
Staff	Personal details, qualifications, payroll, DBS, safeguarding training, attendance, medical records (where relevant)	Employment management, payroll, safeguarding	Legal Obligation / Contract	Health data, vetting data	Payroll provider, LA, DBS, DfE	6 years post-employment	HR system with MFA; encrypted drives
Volunteers / Governors	Contact details, DBS status, training, declarations of interest	Governance, safeguarding, communication	Legal Obligation / Consent	DBS data (criminal data)	DBS, LA, DfE	6 years post-role	Secure digital storage, limited access
Visitors / Contractors	Name, contact info, vehicle registration, ID photo	Site security, safeguarding,	Legal Obligation / Legitimate	N/A	None beyond school security	3 months	Visitor log system; restricted

Category of Data Subject	Type of Personal Data Processed	Purpose of Processing	Lawful Basis (Article 6)	Special Category Data (Article 9)	Data Sharing / Recipients	Retention Period	Security Measures
		health & safety	Interest		logs		view access
Safeguarding Records	Pupil and family personal data, case notes, CPOMS entries	Safeguarding and child protection	Legal Obligation / Vital Interests	Health and welfare data	LA safeguarding teams, police, NHS	Up to age 25 (per KCSIE & IRMS)	CPOMS system, DSL-controlled access
Health & Medical	Medical conditions, allergies, care plans, medication logs	Supporting pupil welfare and inclusion	Vital Interests / Legal Obligation	Health data	NHS professionals, parents	Until pupil leaves school	Locked cabinets and encrypted digital records
CCTV & Site Security	Video footage, timestamps, vehicle registration	Site safety, behaviour management, crime prevention	Legitimate Interest / Public Task	N/A	Police (if required)	30 days (unless required for investigation)	Secure DVR storage, restricted access
Photos / Media	Images, video, pupil names (where consent given)	Celebrating achievement, school publicity, website use	Consent	N/A	School website, social media, press (if agreed)	Until consent withdrawn / pupil leaves	Controlled media library; image consent list
ICT Usage / Monitoring	Network logins, browsing history, filtering alerts	Safeguarding, system security	Public Task / Legal Obligation	N/A	RM SafetyNet, DSL, Online Safety Lead	1 year rolling logs	RM SafetyNet, firewalls, audit logs
Assessment Data	Marks, grades, teacher comments, reports	Monitoring progress and	Public Task	N/A	DfE, LA, parents	7 years after pupil leaves	MIS encryption, restricted role-

Category of Data Subject	Type of Personal Data Processed	Purpose of Processing	Lawful Basis (Article 6)	Special Category Data (Article 9)	Data Sharing / Recipients	Retention Period	Security Measures
		attainment					based access
Financial / Payroll Data	Salary, tax, NI, bank details	Payment of wages and statutory returns	Contract / Legal Obligation	N/A	Payroll provider, HMRC	6 years	Payroll system, encryption, MFA
Alumni Records	Contact details, history, achievements	Maintaining alumni contact and fundraising	Consent	N/A	None without consent	Until consent withdrawn	Separate secure alumni database
Third-Party Platforms	Usernames, activity logs, email, class assignments (e.g. Microsoft 365, Google Workspace)	Learning management, collaboration	Public Task / Consent (where needed)	N/A	Platform provider (data processing agreements in place)	Active use + 1 year post-use	MFA, DPA agreements, UK data hosting where possible

Appendix B - St Vincent's School – Privacy Notices (2025 Edition)

1. Privacy Notice for Pupils

(A child-friendly version should also be produced in accessible formats such as large print, audio or Braille.)

What information we collect

- Your name, address, date of birth and contact details
- Information about your education, attendance, progress and behaviour
- Details about your health, medical conditions and any additional learning or sensory needs
- Photographs, video and recordings (where consent has been given)
- Network login and online-safety monitoring data (RM SafetyNet logs)

Why we collect it

- To help you learn and achieve your full potential
- To keep you safe and healthy while you are in our care
- To record and report your progress to your parents or carers
- To meet legal duties placed on the school by the government

The lawful basis for using your data

We collect and use information because it is **necessary for our public task** of providing education and because we must meet **legal obligations** under education and safeguarding law.
For photographs, trips and optional activities we ask for **consent**.

Who we share information with

- The Department for Education (DfE) and the Local Authority
- Health services such as school nurses or therapists
- Other schools or colleges when you move on
- The police or social-care services if we have a safeguarding concern
- Providers of online learning platforms used in school

How long we keep your data

We keep pupil records until **your 25th birthday** (for safeguarding) and then securely delete them following the IRMS retention schedule.

Your rights

You have the right to ask for a copy of your information, to ask us to correct mistakes, and in some cases to ask us to delete data.
If you are worried about how your data is used, you can speak to your teacher, the **Designated Safeguarding Lead (Mr David Swanston)**, or contact our **Data Protection Officer (DPO)**.

2. Privacy Notice for Parents and Carers

What we collect

- Names, addresses, phone numbers and email addresses
- Relationship to pupil and any parental responsibility information
- Correspondence between home and school
- Records of payments, consents and communications

Why we collect it

- To contact you in emergencies or about your child's progress
- To meet our statutory duties for education and safeguarding
- To organise trips, activities and school events
- To provide support, advice and welfare services

The lawful basis

Processing is mainly carried out as part of our **public task** and to meet **legal obligations** under the Education Acts and safeguarding legislation.
Certain uses (e.g. marketing, photos on website) rely on your **consent**.

Who we share it with

- The DfE and Local Authority
- Health and social-care partners
- School catering and trip providers (where necessary)
- Third-party educational software providers under strict contracts

Retention and security

Parent/carer data is retained for **one year after the pupil leaves** unless required longer by law.
All electronic records are stored on encrypted systems and access is limited to authorised staff.

Your rights

You can request access to, correction or deletion of your data.
Contact the **DPO** or write to the **School Office** for a Subject Access Request form.

3. Privacy Notice for Staff, Volunteers and Governors

Information we hold

- Name, address, contact details, next of kin
- Employment history, qualifications, DBS status and references
- Payroll, pension, tax and bank details
- Health information where relevant for absence or workplace adjustments

- Training, appraisal and safeguarding records

Why we process staff data

- To manage employment, payroll and pensions
- To meet safeguarding and safer-recruitment obligations
- To plan staffing, timetables and professional development
- To monitor equal-opportunity commitments
- To maintain a safe working environment

Lawful bases

Processing is necessary for **contract performance**, **legal obligations** (employment and safeguarding law), and the school's **legitimate interests** in managing staff effectively.
Special-category data (health, DBS information) is processed under Article 9(2)(b) and (g) – employment and safeguarding.

Who we share information with

- Payroll and pension providers
- The DfE and Local Authority (for workforce census)
- HMRC and relevant professional bodies
- DBS service, occupational-health and training providers

Retention

Personnel records are kept for **6 years after employment ends** unless legislation requires longer.
DBS information is kept only for the period allowed under DBS Code of Practice.

Security

All HR data is stored on secure, password-protected systems with multi-factor authentication.
Paper files are kept in locked cabinets within restricted areas.

Your rights

You have the right to access, correct or in some cases erase your personal data.
Concerns can be raised with the **DPO** or directly with the **Information Commissioner's Office (ICO)**.

4. Contact Details

Data Controller: St Vincent's School Governing Body
Senior Information Risk Owner (SIRO): Mr Lee Green
Designated Safeguarding Lead (DSL): Mr David Swanston
Online Safety Lead: Mr Steve Irvine
Data Protection Officer (DPO): [Insert DPO name / service provider / email]
ICO Helpline: 0303 123 1113 **Website:** https://ico.org.uk

Appendix C – Template Data Breach Log

DATE	DESCRIPTION OF INCIDENT	TYPE OF DATA INVOLVED	ACTION TAKEN	REPORTED TO ICO?	OUTCOME