PRENTON HIGH SCHOOL FOR GIRLS

DATA PROTECTION POLICY

Contents

purpose 3
Scope 3
Legislative Framework 3
Roles And Responsibilities 3
The Governing Body/Trust Board 3
Headteacher 3
Data Protection Officer (Dpo) 3
Staff Responsibilities 4
Data Protection Principles 4
Lawful Bases For Processing 4
Special Category Data 4
Data Sharing 4
Privacy Information 5
Individual Rights 5
Subject Access Requests 5
Data Protection Complaints 6
Personal Data Breaches 6
Information Security 6
Website, Cookies And Online Services 6
CCTV 6
Photographs And Media 7
Data Processors And Third Parties 7
Records Management And Retention 7
International Transfers 7
Training And Awareness 7
Monitoring And Review 7

Date of Review:	Summer 2026
Date Ratified:	Summer 2026
Next Review:	Summer 2028

PURPOSE

Prenton High School for Girls is committed to protecting the rights and freedoms of individuals and ensuring that personal information is processed lawfully, fairly and securely.

This policy establishes the framework through which the School complies with UK data protection legislation and demonstrates accountability for the personal information it processes.

SCOPE

This policy applies to:

- students;
- parents and carers;
- employees;
- governors and trustees;
- volunteers;
- contractors;
- agency workers;
- visitors; and
- any other individual whose personal information is processed by the School.

The policy applies to all personal data regardless of format, including paper records, electronic records, images, CCTV footage and email communications.

LEGISLATIVE FRAMEWORK

This policy operates in accordance with:

- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018;
- Data (Use and Access) Act 2025;
- Freedom of Information Act 2000;
- Environmental Information Regulations 2004;
- Human Rights Act 1998;
- Education Act 1996;
- Education Act 2002;
- Keeping Children Safe in Education;
- relevant safeguarding legislation and statutory guidance.

ROLES AND RESPONSIBILITIES

The Governing Body/Trust Board

The Board has overall responsibility for ensuring compliance with data protection legislation.

Headteacher

The Headteacher has operational responsibility for ensuring implementation of this policy.

Data Protection Officer (DPO)

The School's Data Protection Officer is:

Mrs H Sanderson
Email: sandersonh@prentonhighschool.co.uk

The DPO is responsible for:

- advising on data protection compliance;
- monitoring compliance activities;
- supporting data protection impact assessments;
- handling data protection complaints;

DRAFT

- managing data subject rights requests;
- acting as a point of contact with the Information Commissioner's Office (ICO).

Staff Responsibilities

- All staff must:
- comply with this policy;
- complete required training;
- maintain confidentiality;
- report data breaches promptly;
- process personal data only where authorised.

DATA PROTECTION PRINCIPLES

- The School shall ensure personal data is:
- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary;
- accurate and kept up to date;
- retained only as long as necessary;
- processed securely using appropriate technical and organisational measures.

The School will also demonstrate accountability for compliance with these principles.

LAWFUL BASES FOR PROCESSING

The School will only process personal information where a lawful basis exists under Article 6 UK GDPR.

These may include:

- Legal Obligation;
- Public Task;
- Contract;
- Vital Interests;
- Legitimate Interests;
- Consent.

Where consent is relied upon it must be freely given, informed and capable of being withdrawn.

SPECIAL CATEGORY DATA

Special category information may include:

- health information;
- disability information;
- ethnicity;
- religion or belief;
- biometric data;
- trade union membership;
- safeguarding information.

Such information will only be processed where an additional condition under Article 9 UK GDPR and Schedule 1 Data Protection Act 2018 applies.

DATA SHARING

The School may share information where lawful and necessary with:

- Department for Education;
- Local Authorities;
- examination boards;
- safeguarding partners;

DRAFT

- NHS organisations;
- social care agencies;
- police and law enforcement bodies;
- courts and tribunals;
- auditors;
- insurers;
- legal advisers;
- contracted service providers.

Before sharing information, the School will consider:

- whether there is a lawful basis;
- necessity and proportionality;
- security arrangements;
- data minimisation requirements.

PRIVACY INFORMATION

The School will provide clear privacy notices explaining:

- what information is collected;
- why it is processed;
- lawful bases relied upon;
- who information is shared with;
- retention periods;
- individual rights.

Separate privacy notices are maintained for:

- students and parents/carers;
- staff, governors, volunteers and contractors.

INDIVIDUAL RIGHTS

Individuals may have the right to:

- be informed;
- access their personal information;
- request rectification;
- request erasure;
- request restriction;
- object to processing;
- data portability;
- withdraw consent;
- challenge automated decision-making.

Requests should be directed to the DPO.

SUBJECT ACCESS REQUESTS

Individuals may request access to personal information held about them.

The School will respond within one calendar month unless an extension is permitted under legislation.

The School maintains a record of:

- requests received;
- responses issued;
- exemptions applied;
- outcomes.

Further information is contained within the Subject Access Request Procedure.

DRAFT

DATA PROTECTION COMPLAINTS

The School operates an internal data protection complaints process.

Complaints relating to the collection, use, disclosure, retention, security or accuracy of personal information should be submitted to the DPO.

The School will:

- acknowledge complaints;
- investigate concerns;
- provide a written response;
- maintain records of complaints and outcomes.

Where a complainant remains dissatisfied, they may complain to the Information Commissioner's Office.

PERSONAL DATA BREACHES

A personal data breach means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

All staff must report suspected breaches immediately.

The DPO will:

- assess the risk;
- maintain a breach register;
- determine whether notification is required;
- notify the ICO within 72 hours where legally required;
- notify affected individuals where necessary.

INFORMATION SECURITY

The School will implement appropriate security measures including:

- password controls;
- access controls;
- encryption where appropriate;
- secure disposal procedures;
- secure storage of records;
- cyber security measures;
- business continuity arrangements.

WEBSITE, COOKIES AND ONLINE SERVICES

The School website will include:

- privacy notices;
- accessibility information;
- cookie information;
- statutory publications.

Cookies and online tracking technologies will be managed in accordance with applicable legal requirements.

CCTV

The School operates CCTV systems for safeguarding, security and crime prevention purposes.

The School will:

- display appropriate signage;
- limit access to recordings;
- retain footage only for as long as necessary;
- comply with ICO guidance relating to surveillance systems.

DRAFT

CCTV footage will normally be retained for up to three months unless required for an investigation or legal proceedings.

PHOTOGRAPHS AND MEDIA

The School may use photographs and video recordings for educational, safeguarding, promotional and administrative purposes.

Where consent is required, it will be obtained and recorded.

The School will maintain appropriate controls over the storage, use and publication of images.

DATA PROCESSORS AND THIRD PARTIES

Where external organisations process personal information on behalf of the School:

- written agreements will be in place;
- processors will provide sufficient guarantees of compliance;
- security requirements will be monitored;
- processing instructions will be documented.

The School remains responsible for ensuring compliance with UK GDPR requirements.

RECORDS MANAGEMENT AND RETENTION

Personal information will be retained in accordance with the School's Records Retention Schedule.

Records will be:

- retained only for as long as necessary;
- reviewed periodically;
- securely destroyed when no longer required.

INTERNATIONAL TRANSFERS

Where personal information is transferred outside the United Kingdom, appropriate safeguards will be implemented in accordance with UK GDPR requirements.

TRAINING AND AWARENESS

The Headteacher will ensure that staff receive appropriate data protection training.

Training will include:

- induction training;
- refresher training;
- breach reporting procedures;
- safeguarding and confidentiality requirements.

MONITORING AND REVIEW

This policy will be reviewed annually or sooner where legislative, regulatory or operational changes require.

Compliance with this policy may be monitored through audits, reviews and investigations.

DRAFT