Horningsham Primary School

Church Street, Horningsham, Warminster, Wiltshire, BA12 7LW

Tel: 01985 844342 Email: admin@horningsham.wilts.sch.uk

Headteacher: Mrs Odele Lapham

Data Protection Policy

Introduction

Horningsham Primary School ("the School") collects, uses, and controls personal information about staff, pupils, parents, and other individuals who have contact with the school. This information is necessary to enable the provision of education and other associated functions. Additionally, there may be a legal requirement to collect and use information to ensure compliance with statutory responsibilities.

The School is the Data Controller under the Data Protection Act 2018 (DPA), the UK General Data Protection Regulation (UK GDPR) as amended by the Data Protection and Digital Information Act 2024 (DUAA), and other relevant legislation.

The School is registered with the **Information Commissioner's Office (ICO)**, detailing the information held and its use. These details, along with our Data Protection Officer (DPO), are available on the ICO's website.

Our **Data Protection Officer (DPO)** is Jeremy Shatford. He may be contacted in writing to the school (clearly marked "Data Protection") or by email at **dpo@jeremyshatford.co.uk** .

Purpose

This policy ensures that personal information is handled correctly, securely, and lawfully in accordance with:

- The **Data Protection Act 2018**
- The **UK GDPR (as amended by the DUAA 2024)**
- The **Freedom of Information Act 2000 (FOI)**
- Any other relevant legislation or statutory guidance.

It applies to all personal data processed by the school, whether collected, recorded, stored, shared, or destroyed — in electronic or paper format.

All staff involved with the collection, processing, and disclosure of personal data will be made aware of their duties and responsibilities to adhere to this policy.

Governance

The governing body has overall responsibility for data protection compliance.

This policy will be reviewed annually and updated as required to reflect legislative or operational changes, including updates issued under the DUAA.

Records and Documentation

The School will maintain all required records under Article 30 UK GDPR, including:

- Privacy notices
- Record of processing activities (ROPA)
- Data sharing agreements
- Data protection impact assessments (DPIAs)

- Details of security measures
- Retention schedules
- Details of data processors and third-party services

Under the DUAA, the School may rely on **proportionate record-keeping**, reflecting the scale and nature of processing, while still demonstrating compliance.

What is Personal Data?

Personal data means any information relating to an identified or identifiable individual. This includes names, contact details, pupil assessment data, staff employment information, health records, photographs, and other identifiers such as IP addresses or biometric data.

Certain data is classed as **special category data**, requiring additional protection, including data revealing racial or ethnic origin, political opinions, religious beliefs, health, genetic or biometric data, or sexual orientation.

Accountability and Governance

The School demonstrates accountability by:

- Maintaining up-to-date data protection documentation and contracts;
- Embedding data protection by design and by default;
- Conducting DPIAs where risks are identified;
- Maintaining a record of personal data breaches;
- Reviewing and updating privacy notices annually;
- Appointing a Data Protection Officer (DPO).

Under the DUAA, organisations must also ensure **appropriate senior-level oversight** and be able to demonstrate **active compliance** with data protection law.

The Data Protection Principles

The School upholds the seven UK GDPR principles (Article 5), including those clarified under the DUAA:

- **Lawfulness, fairness, and transparency** – Data must be processed lawfully and fairly.
  - The School primarily relies on the **public task** lawful basis for most processing (e.g. education, safeguarding, assessment).
  - For activities outside statutory duties (e.g. optional school photography, alumni engagement), **recognised legitimate interests** may be used where appropriate.
- **Purpose limitation** – Data will be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
- **Data minimisation** – Only adequate, relevant, and necessary data will be collected.
- **Accuracy** – Personal data will be accurate and, where necessary, kept up to date.
- **Storage limitation** – Data will not be kept longer than necessary.
- **Integrity and confidentiality (security)** – Appropriate technical and organisational security measures will be applied.
- **Accountability** – The School must be able to demonstrate compliance with all principles.

Lawful Bases for Processing

Under the UK GDPR and DUAA, the lawful bases for processing are:

- **Public Task** – Most of the School's processing is necessary for the performance of tasks carried out in the public interest or under official authority (e.g. education, safeguarding).
- **Legal Obligation** – Processing to comply with statutory duties (e.g. attendance returns, payroll reporting).
- **Contract** – Processing necessary for employment or service contracts.
- **Consent** – For optional or non-statutory activities (e.g. use of pupil photos for publicity).
- **Vital Interests** – To protect someone's life (e.g. medical emergency).
- **Recognised Legitimate Interests** – Under the DUAA, public authorities **may rely on legitimate interests** where processing is not carried out in performance of a public task, and where the processing is necessary and proportionate (e.g. staff wellbeing initiatives, communications with alumni, or school marketing events).

Rights of Individuals

Individuals have the following rights, which the DUAA maintains and clarifies:

- To be informed
- To access their data (Subject Access Requests)
- To rectification
- To erasure ("right to be forgotten")
- To restrict processing
- To data portability (where applicable)
- To object
- To challenge automated decision-making and profiling

The DUAA also confirms individuals' right to **human review of significant automated decisions**, including those involving AI.

Fair Processing and Data Sharing

Privacy Notices are issued to pupils, parents, and staff, explaining:

- What data is collected and why
- The lawful basis for processing
- Who it is shared with and how long it is retained

Data will only be shared when lawful to do so — usually under **public task**, **legal obligation**, or **contractual necessity**.

The School will ensure appropriate **data sharing agreements** are in place with third-party processors and that **due diligence** is carried out before data is transferred.

Under the DUAA, the School must also ensure appropriate safeguards are in place when using **AI or automated systems** to process personal data.

Information Security

The School implements technical and organisational security measures, including:

- Restricted physical access to records and ICT systems
- Encryption and password protection
- Regular review of user access levels
- Staff training on cyber security and phishing awareness
- Secure disposal of devices and paper records
- Adherence to NCSC and DfE cybersecurity guidance

Data Breach Response

All staff must report personal data breaches immediately to the DPO.

The School will:

- Contain and assess the breach;
- Record it in the breach register;
- Notify the ICO within 72 hours if there is a risk to individuals' rights and freedoms;
- Inform affected individuals where appropriate.

Contractors and Processors

All suppliers and contractors processing personal data on behalf of the School must:

- Have a written contract in place (Article 28 UK GDPR);
- Demonstrate adequate security measures;
- Process data only on the School's documented instructions;
- Assist in fulfilling data protection obligations (e.g. SARs, breach management).

Training and Awareness

All staff, governors, and contractors handling personal data receive training at induction and regular refresher training thereafter. The School promotes a culture of ongoing GDPR awareness and accountability.

Monitoring and Review

This policy will be reviewed annually or sooner if legislation or guidance changes. The School will monitor compliance through audits and staff feedback.

Contacts

For questions about this policy or data protection matters:

The School Office: admin@horningsham.wilts.sch.uk

Data Protection Officer: dpo@jeremyshatford.co.uk

Further information and advice:

Information Commissioner's Office (ICO) – https://ico.org.uk / Tel: 0303 123 1113

Related Policies

- Freedom of Information Publication Scheme
- Privacy Notices
- Subject Access Request Procedure
- Data Breach Policy
- Retention Schedule
- Online Safety Policy
- Staff Acceptable Use Agreement
- Safeguarding and Child Protection Policy

Document History

Date	Description
01/05/2024	Complete revision
22/10/2025	Updated for DUAA and UK GDPR 2024–25 compliance

Last Updated: October 2025