Horningsham Primary School

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

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

Headteacher: Mrs Odele Lapham

Data Breach Response Policy

Introduction

Horningsham Primary School ("the School") is committed to protecting all personal data in compliance with the **UK General Data Protection Regulation (UK GDPR)**, the **Data Protection Act 2018**, and relevant **Department for Education (DfE)** guidance.

This Data Breach Response Plan sets out the process to be followed in the event of a personal data breach to minimise risk, ensure a timely and effective response, and comply with all legal and regulatory obligations.

Definition of a Data Breach

A personal data breach is a **security incident** that results in any of the following:

- Unauthorised access to, or disclosure of, personal data.
- Accidental or unlawful destruction, loss, alteration, or theft of personal data.
- Unavailability of personal data due to system failure, cyberattack, or ransomware.

A breach may be **accidental or deliberate** and can occur in both digital and paper-based records.

Roles and Responsibilities

Data Protection Officer (DPO) – The DPO acts independently to advise on data protection compliance. The DPO must be informed **immediately** of all suspected or confirmed data breaches. The DPO will:

- Advise on the assessment and containment of the breach.
- Determine whether the incident is reportable to the ICO and assist with the notification process.
- Maintain oversight of the incident record and ensure lessons learned are implemented.

Headteacher: Leads the breach response, liaising with the DPO and Governing Body as appropriate. Ensures staff cooperation and communication with relevant stakeholders.

Admin and Finance Officer: Supports incident investigation and documentation, ensures corrective actions are completed, and maintains the breach register.

IT Support: Identifies technical causes, assists with containment, and implements measures to prevent recurrence.

All Staff: Must immediately report any suspected or actual breach to the Headteacher and DPO, cooperate with investigations, and follow instructions to mitigate risk.

Breach Detection and Reporting

Any staff member who becomes aware of a potential or confirmed data breach must report it immediately to the Headteacher and DPO.

A Data Breach Reporting Form must be completed as soon as possible, providing all known details.

If IT systems are involved, the school's IT provider must be contacted without delay to assist in assessing and containing the incident.

Initial Assessment

The DPO and Headteacher will carry out a preliminary assessment to determine:

- The nature and cause of the breach.
- Categories and volume of personal data affected.
- Number and type of individuals affected.
- The potential impact on individuals (e.g., identity theft, financial loss, distress, reputational harm).
- Any immediate containment and recovery actions required.

Containment and Mitigation

Actions may include:

- Stopping unauthorised access (e.g., disabling accounts, retrieving misdirected emails).
- Recovering or securing lost data (e.g., restoring backups, retrieving physical documents).
- Resetting passwords or increasing access controls.
- Implementing temporary or permanent technical fixes.
- Ensuring affected systems are monitored for further risks.

Notification to the ICO

If the breach is **likely to result in a risk to the rights and freedoms of individuals**, the DPO must report it to the **Information Commissioner's Office (ICO)** within **72 hours** of becoming aware of the breach.

The report must include:

- Nature and circumstances of the breach.
- Categories and volume of data and individuals affected.
- Likely consequences for individuals.
- Steps taken or proposed to address the breach and mitigate harm.
- Contact details for the DPO.

7.3 If the notification is delayed beyond 72 hours, the reason for the delay must be recorded and included in the report.

Notification to Affected Individuals

Where the breach is high risk, affected individuals must be informed without undue delay.

The DPO must be consulted before any notification is issued.

The communication should include:

- A clear description of the breach.
- The likely consequences for the individual.
- Steps the school has taken and any actions the individual should take (e.g., changing passwords, being alert to phishing).
- Contact details for further advice and support (usually the DPO).

Notification to Other Relevant Bodies

Depending on the nature of the breach, the School may also need to notify:

- **Local Authority** – where required under data-sharing or service agreements.
- **Department for Education (DfE)** – where incidents meet reporting criteria.
- **Police** – if criminal activity (e.g., theft or hacking) is suspected.
- **Parents/Guardians** – if a breach affects pupils, parents or carers directly.

Documentation and Review

All breaches, regardless of severity or reporting outcome, must be recorded in the **School's Data Breach Register**. Each record must include:

- Date and time of detection and report.
- Description of the breach and affected data.
- Details of actions taken and mitigation measures.
- Assessment of whether the ICO or individuals were notified and why.
- Lessons learned and actions taken to prevent recurrence.

The DPO will periodically review the breach register to identify recurring issues and recommend improvements to practice or policy.

Post-Breach Actions and Preventive Measures

Following a breach, the School will:

- Conduct a **root cause analysis** to determine how the breach occurred.
- Implement appropriate **technical or organisational measures** to prevent recurrence.
- Review and, if necessary, update relevant policies and staff training.
- Provide follow-up reports to the Governing Body and relevant authorities if required.

Training and Awareness

- All staff will receive **mandatory data protection and breach response training** at induction.
- Refresher training will be provided **annually** or more frequently if required.
- Periodic updates and awareness reminders will be provided to reinforce good data protection practices.
- Training completion will be recorded and monitored by the Admin and Finance Officer.

Contact Details

For reporting or advice relating to data breaches:

Data Protection Officer: dpo@jeremyshatford.co.uk

Last Updated: October 2025