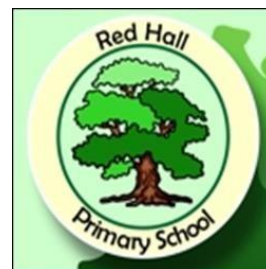


Red Hall Primary School

Data Protection Policy



Document History	
Originally Written:	May 2018
Updated:	September 2024 - MD September 2026
By:	Andrea James
Approved by Governing Body:	21 st September 2026
Next Review Date:	September 2027

1.0 – Introduction:

1.1 - This Data Protection Policy ensures compliance with the **UK General Data Protection Regulation (UK GDPR)**, the **Data Protection Act 2018 (DPA 2018)**, the **Data (Use and Access) Act 2025**, and all associated legislation. It incorporates guidance from the **Information Commissioner's Office (ICO)**.

1.2 - The DPA 2018 and UK GDPR give individuals rights over their personal data and protect them from misuse, loss, or unauthorised access.

1.3 - Red Hall Primary School is registered with the ICO as a **Data Controller** and is responsible for ensuring all processing of personal data is lawful, fair, and transparent.

2.0- Purpose:

2.1 - This Policy outlines how the school complies with the DPA 2018 and UK GDPR, ensuring personal data is processed lawfully, securely, and responsibly.

2.2 - The Policy sets out the school's approach to data protection, including responsibilities, rights of individuals, and expectations for staff, students, and third parties.

3.0- Scope:

3.1 - This Policy applies to all employees (including temporary, casual or agency staff and contractors, consultants and suppliers working for, or on behalf of, the school), third parties and others who may process personal information on behalf of the school.

3.2 - The Policy also applies to staff and students involved in research or professional practice activities requiring access to personal data. Relevant departments must ensure compliance and provide appropriate guidance.

4.0- Data covered by the policy:

4.1 - Personal data includes any information relating to an identifiable individual, whether held electronically or in structured paper files.

4.2 - Special category data includes:

- Racial or ethnic origin
- Political opinions
- Religious or similar beliefs
- Trade union membership
- Physical or mental health

- Sexual orientation
- Biometric or genetic data

Processing special category data requires additional safeguards and a lawful basis under UK GDPR.

5.0- The Six Data Protection Principles:

5.1 - Under UK GDPR, personal data must be:

- **Lawfully, fairly, and transparently processed**
- **Collected for specified, explicit, and legitimate purposes**
- **Adequate, relevant, and limited** to what is necessary
- **Accurate and kept up to date**
- **Stored no longer than necessary**
- **Processed securely**, protecting against unauthorised access, loss, or damage

6.0- Responsibilities:

6.1 - The school has appointed a **Data Protection Officer (DPO)** to oversee compliance, provide guidance, and manage data protection concerns.

6.2 - All new staff must complete mandatory information governance training. Existing staff must undertake regular refresher training.

6.3- Employees of the School are expected to:

- Familiarise themselves and comply with the six data protection principles
- Ensure any possession of personal data is accurate and up to date
- Ensure their own personal information is accurate and up to date
- Keep personal data for no longer than is necessary

- Ensure that any personal data they process is secure and in compliance with the school's information related policies and strategies.
- Acknowledge data subjects' rights (e.g. right of access to all their personal data held by the school) under the DPA 2018, and comply with access to records
- Ensure personal data is only used for those specified purposes and is not unlawfully used for any other business that does not concern the school.
- "Obtain consent **where required** when collecting, sharing or disclosing personal data".
- Contact the DPO at DPO@redhall.darlington.sch.uk or any concerns or doubt relating to data protection to avoid any infringements of the DPA 2018.

6.4- Students must comply with School security procedures and respect data protection principles.

7.0- Obtaining, Disclosing and Sharing:

7.1 - Only data necessary for a legitimate School purpose should be collected.

7.2 - Students and parents/carers are informed about data processing through the **Privacy Notice** provided at registration. The school processes pupil data under the lawful bases of **legal obligation** and **public task** as set out in Article 6 of the UK GDPR. The school does not rely on consent as the primary lawful basis for processing pupil data.

7.3 - Staff are informed about data processing through the **Staff Privacy Notice** provided upon employment. The school processes staff data under the lawful bases of **contract**, **legal obligation**, and **legitimate interests** as set out in Article 6 of the UK GDPR.

7.4 - All personal data must be collected, stored, and processed securely.

7.5 - Personal information must not be disclosed to a third-party organisation without prior consent of the individual concerned unless the disclosure is legally required or permitted. This also includes information that would confirm whether or not an individual is or has been an applicant, student or employee of the school.

7.5 - Personal information must not be disclosed to a third-party organisation without prior consent of the individual concerned unless the disclosure is legally required or permitted. This also includes information that would confirm whether or not an individual is or has been an applicant, student or employee of the school.

7.6 - Regular data sharing with third parties must be governed by a **written Data Sharing Agreement**. Ad hoc sharing must comply with UK GDPR.

7.7 - The school may have a duty to disclose personal information in order to comply with legal or statutory obligation. The DPA 2018 allows the disclosure of personal data to authorised bodies, such as the police and other organisations that have a crime prevention or law enforcement function. Any requests to disclose personal data should be directed to the Headteacher.

7.8- Data Protection and Safeguarding:

7.8 (1) - The School recognises that effective safeguarding requires appropriate information sharing. Where there are safeguarding concerns about a child, staff must share information in line with the School's Child Protection and Safeguarding Policy and statutory guidance in Keeping Children Safe in Education.

7.8 (2) - Data protection legislation does not prevent the sharing of information for the purposes of keeping children safe. Staff should not let data protection concerns stand in the way of promoting the welfare and protecting the safety of children.

8.0- Retention, Security and Disposal:

8.1 - Recipients responsible for the processing and management of personal data need to ensure that the data is accurate and up-to-date. If an employee, student or applicant is dissatisfied with the accuracy of their personal data, then they must inform the Office Manager.

8.2 - Data must not be retained longer than necessary and must follow the **School's Retention Schedule**.

8.3 - Staff must ensure secure storage and prevent accidental loss or damage.

8.4 - In accordance with the School's Flexible Working Scheme, staff working from home will be responsible for ensuring that personal data is stored securely and is not accessible to others.

8.5 - All departments should ensure that data is destroyed in accordance with the Retention Schedule when it is no longer required.

8.6 - Paper data must be shredded or placed in confidential waste. Electronic data must be securely deleted. Hardware must be degaussed or securely wiped by the IT provider.

9.0- Transferring Personal Data:

9.1 - Any transfer of personal data must be completed securely in line with the School's Information Security Policy.

9.2 - External emails containing personal data must be encrypted and password-protected.

9.3 - Care should be taken to ensure emails containing personal data are not sent to unintended recipients. It is important that emails are addressed correctly and care is taken when using reply all or forwarding or copying others in to emails. Use of the blind copy facility should be considered when sending an email to multiple recipients to avoid disclosing personal information to others.

9.4 - Personal email accounts must not be used for School-related personal data.

10.0- Data Subjects Right of Access (SARs):

10.1 - Individuals have the right to access their personal data.

10.2 - The school encourages informal access where appropriate but maintains a formal SAR Procedure.

10.3 – Requests must be submitted via a SAR form to:

DPO@redhall.darlington.sch.uk.

10.4 – The school will respond in one month of receiving a valid request and proof of identity. No fee will be charged.

11.0- Reporting a Data Security Breach:

11.1 – Any breach (loss, theft, unauthorised access, system failure) must be reported immediately to the DPO. IT-related breaches must also be reported to the Headteacher and the IT provider.

11.2 – Breaches will be investigated under the school's Data Breach Policy. Serious breaches may require reporting to the ICO within **72 hours**, in line with UK GDPR.

