Rainow Primary School

Caring, Learning, Achieving.

Data Protection Policy

Member of staff responsible:	**School Business Manager /**
Date approved:	**Spring 2026**
Date to be reviewed:	***Spring 2029**

**or in light of legal or school-level changes*

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, volunteers, visitors and other individuals is collected, stored and processed in accordance with the UK GDPR and the Data Protection Act 2018. This policy applies to all personal data, regardless of whether it is in paper or electronic form.

2. Legislation and guidance

This policy meets the requirements of: UK GDPR, Data Protection Act 2018, ICO guidance, IRMS Records Management Toolkit for Schools (2024), and the Education (Pupil Information) (England) Regulations 2005.

3. Definitions

Personal data: Any information identifying an individual.
Special category data: Sensitive information requiring extra protection, such as racial origin, political opinions, religious beliefs, trade union membership, health data, genetics, biometrics, and sexual orientation.
Processing: Any operation applied to personal data.
Data subject: The individual the data relates to.
Data controller: Rainow Primary School.
Data processor: Any third-party processing data on behalf of the school.
Personal data breach: A breach of security resulting in loss, alteration, unauthorised disclosure or access to personal data.

4. The Data Controller

Rainow Primary School acts as the data controller for all personal data processed. The school is registered with the Information Commissioner's Office (ICO) and renews its registration annually or as required. The school determines the purpose and lawful basis for processing personal data and ensures that all processing complies with UK GDPR and the Data Protection Act 2018.

5. Roles and Responsibilities

This policy applies to all staff, governors, volunteers, contractors, and external organisations operating on behalf of the school. All individuals are responsible for ensuring that personal data is handled safely.

Governing Board: Ensures overall compliance with data protection law.

Data Protection Officer (DPO): Oversees compliance, provides advice, monitors processes, and acts as point of contact for the ICO and data subjects.

Headteacher: Acts as the data controller's representative and ensures implementation of this policy.

All Staff: Must follow data protection principles, attend required training, report breaches, and consult the DPO when unsure about lawful data handling.

6. Data Protection Principles

Under UK GDPR, personal data must be processed according to six key principles:

- Lawfulness, fairness, transparency – data must be processed legally and openly.
- Purpose limitation – data collected for one purpose cannot be used for another without a lawful basis.
- Data minimisation – only the minimum necessary data should be collected.
- Accuracy – data must be kept accurate and up to date.
- Storage limitation – data must not be kept longer than necessary.
- Integrity and confidentiality – data must be secured against loss, damage, or unauthorised access.

Rainow Primary School is committed to ensuring compliance with all six principles.

7. Collecting Personal Data

7.1 Lawfulness, Fairness and Transparency

We will only process personal data when a lawful basis applies. These include: public task, legal obligation, vital interests, contract, consent, and legitimate interests (used rarely in schools). Special category data requires an additional processing condition under the DPA 2018.

We provide privacy notices to all pupils, parents, staff and visitors explaining what data we collect and why.

7.2 Limitation, Minimisation and Accuracy

Personal data is collected only for clear and legitimate purposes. Staff may only access personal data needed to perform their role. Data that is no longer required is securely deleted or anonymised in accordance with the IRMS Records Management Toolkit for Schools (2024).

8. Sharing Personal Data

We will not routinely share personal data with third parties unless it is lawful and necessary. Data may be shared where:

- A safeguarding or welfare concern exists.
- External agencies require information to support education, health, or care.

- Contractors or service providers need data to deliver a school service (e.g., IT systems). All processors must comply with UK GDPR and data sharing agreements.
- We are legally required to share data with authorities such as the DfE, police, or courts.

Only the minimum necessary information will be shared, and international transfers will only occur where UK GDPR safeguards exist.

9. Subject Access Requests and Individual Rights

Under UK GDPR, individuals have rights regarding their personal data.

9.1 Subject Access Requests (SARs)

Individuals may request access to their personal data. Requests must be forwarded immediately to the DPO. We may verify identity and must respond within one month unless an extension applies.

9.2 Children and SARs

A child's personal data belongs to the child. Parents may make a request only where the child cannot understand their rights (typically under age 12 but assessed individually).

9.3 Responding to SARs

We may refuse or charge a fee for unfounded or excessive requests. Information may be withheld if disclosure:

- Risks harm to the individual.
- Reveals safeguarding concerns.
- Involves adoption or court-related data.

9.4 Other Rights

Individuals may request rectification, erasure, restriction, objection to processing, data portability, withdrawal of consent, and the right to object to automated decision-making. All requests must be referred to the DPO.

10. Parental Requests to See the Educational Record

Parents with parental responsibility may request access to their child's educational record. The school must provide this within 15 school days, free of charge, in accordance with the Education (Pupil Information) (England) Regulations 2005.

11. Photographs and Videos

Photographs and videos may be taken for educational, promotional, or celebratory purposes.

- Written parental consent is obtained for use in displays, publications, websites, and approved online platforms.
- Consent may be withdrawn at any time.
- Images will not be accompanied by identifying information unless necessary and consented.
- Parents taking photos at events are asked not to upload images of children to social media, although the school cannot enforce this.

- All images are processed securely and in line with the school's safeguarding and online safety duties.

12. Data Protection by Design and Default

We integrate data protection principles into all processing activities. Measures include:

- Appointing a trained Data Protection Officer (DPO).
- Conducting Data Protection Impact Assessments (DPIAs) for high-risk activities or new technologies.
- Ensuring all systems and processes support confidentiality, integrity, and availability of data.
- Embedding data protection requirements into procurement, onboarding of systems, and contracts.
- Maintaining appropriate documentation including Records of Processing Activities (ROPA).
- Ensuring staff are trained and confident in the principles of data minimisation and purpose limitation.

13. Data Security and Storage of Records

We take appropriate organisational and technical measures to protect personal data. These include:

- Secure storage of paper records in locked areas.
- Password-protected and encrypted devices for electronic data.
- Clear desk and screen practices.
- Strong password protocols and two-factor authentication where available.
- Restricted access to data based on job role.
- Secure email when transferring sensitive data (e.g., Egress for safeguarding information).
- Due diligence on third-party providers to ensure compliance with UK GDPR.
- Confidentiality agreements for volunteers and external professionals.
- Verification processes before personal data is released over the phone.
- Secure transfer of safeguarding records in line with statutory guidance.

Data security is reviewed regularly and strengthened as needed.

14. Disposal of Records

Personal data will be disposed of securely when no longer required, in accordance with the IRMS Records Management Toolkit (2024). This includes:

- Shredding or incinerating paper documents.
- Secure deletion or overwriting of electronic files.
- Using approved contractors who meet UK GDPR destruction standards.

Data that becomes inaccurate or outdated will be rectified or securely destroyed unless a legal requirement prevents this.

15. Personal Data Breaches

A personal data breach is any event leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

All staff must report suspected breaches immediately to the DPO. Delay may increase risk. The DPO will:

- Investigate and assess the breach.
- Contain the breach and reduce potential harm.
- Determine whether the breach must be reported to the ICO within 72 hours.
- Notify affected individuals where the breach poses a high risk to their rights.
- Maintain a breach log for all incidents, whether reported to the ICO or not.

Examples include:

- Sending personal data to the wrong recipient.
- Loss or theft of a device containing unencrypted personal data.
- Unauthorised access to personal information.
- Accidental publication of sensitive data.

16. Training

All staff and governors receive basic training on UK GDPR principles as part of their induction. Additional refresher training is provided regularly and whenever legislative or procedural changes occur.

Staff handling sensitive or high-risk data (e.g., Safeguarding, SEN, Administration, SLT) receive enhanced training.

17. Monitoring Arrangements

The DPO monitors compliance with this policy, oversees training, and ensures regular audits of data handling practices.

This policy will be reviewed every two years or sooner if required by legislative change. The Governing Board must approve all policy updates.

18. Links with Other Policies

This Data Protection Policy links to and should be read alongside the following school policies:

- Data Security Breach Prevention and Management Plan
- Child Protection and Safeguarding Policy
- Online Safety / E-Safety Policy
- Acceptable Use Policy (IT)
- Freedom of Information Publication Scheme
- Images and Videos Parental Consent Form

These policies collectively support the safe, lawful, and transparent handling of personal data.

Appendix 1: Personal Data Breach Procedure

This procedure is based on ICO guidance and outlines how Rainow Primary School manages personal data breaches.

- Any member of staff or data processor who discovers or suspects a breach must immediately notify the DPO.
- The DPO will investigate and determine whether a breach has occurred. This includes reviewing whether data:

– Was lost or stolen

– Was accidentally destroyed or altered

– Was disclosed or accessed by an unauthorised person

- The DPO will assess the risk to individuals, considering potential harm, identity theft, discrimination, or confidentiality breaches.
- If the breach is likely to pose a risk to individuals' rights and freedoms, the DPO will notify the ICO within 72 hours.
- Where there is a high risk to individuals, the DPO will notify affected parties without undue delay.
- The DPO will maintain a full breach record including:

– Facts relating to the breach

– Actions taken

– Measures to prevent recurrence

- The DPO and Headteacher will review the incident and amend procedures or provide further staff training as needed.

Examples of breaches include:

- Sensitive data emailed to the wrong person
- Publication of personal data on an unsecured system
- Loss of unencrypted devices
- Unauthorised access to safeguarding information

This procedure ensures that breaches are managed quickly, transparently, and in compliance with UK GDPR.