Rawdah Montessori Primary School

Data Protection Policy

Version: 1.0

Reviewed: October 2025

Next Review Due: October 2026

1. Policy Statement

Rawdah Montessori Primary School is committed to protecting the privacy and rights of all individuals whose personal data we process. We recognise our legal and ethical responsibility to handle personal information lawfully, fairly, and transparently in accordance with the **UK General Data Protection Regulation (UK GDPR)** , the **Data Protection Act 2018 (DPA 2018)** , and the **Data (Use and Access) Act 2025 (DUAA 2025)** .

As a faith-based school, our Islamic values of honesty, integrity, and respect for others underpin our approach to data protection. We believe that safeguarding personal information is an extension of our duty to protect and respect our community.

This policy sets out the framework for how we collect, use, store, and dispose of personal data relating to pupils, parents, staff, governors, contractors, and visitors. It should be read in conjunction with the:

- **Safeguarding and Child Protection Policy**
- **Subject Access Request Procedure**
- **Social Media and ICT Policy**
- **Staff Code of Conduct**
- **Privacy Notices (for pupils, parents, staff, and website users)**
- **Service Contract with Greensville Trust** (for shared site data processing)

2. Purpose and Aims

The purpose of this policy is to:

- Ensure compliance with all relevant data protection legislation.
- Protect the rights of individuals whose personal data we process.
- Establish clear guidelines for the collection, use, storage, and disposal of personal data.
- Promote transparency and accountability in all data processing activities.
- Safeguard against data breaches and ensure appropriate security measures are in place.
- Provide a framework for responding to data subject requests and complaints.

3. Legal Framework

This policy is guided by the following legislation and guidance:

Legislation / Guidance	Relevance
UK General Data Protection Regulation (UK GDPR)	The primary regulation governing the processing of personal data in the UK.
Data Protection Act 2018 (DPA 2018)	Supplements the UK GDPR and provides additional exemptions and provisions.
Data (Use and Access) Act 2025 (DUAA 2025)	Introduces significant updates, including a new lawful basis ('recognised legitimate interest'), changes to subject access requests, and a formalised complaints process .
Keeping Children Safe in Education (KCSIE 2025)	Emphasises that data protection law supports, rather than hinders, effective safeguarding .
Freedom of Information Act 2000	Governs access to information held by public authorities (where applicable).

Legislation / Guidance	Relevance
Privacy and Electronic Communications Regulations 2003 (PECR)	Governs electronic marketing and cookies (as amended by DUAA 2025) .
Information Commissioner's Office (ICO) Guidance	Sector-specific guidance for education providers on data sharing, subject access requests, and information security .

4. Definitions

Term	Definition
Personal Data	Any information relating to an identified or identifiable natural person ('data subject') .
Special Category Data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership; genetic data; biometric data (where used for identification); health data; or data concerning sex life or sexual orientation .

Term	Definition
Processing	Any operation performed on personal data (e.g., collection, storage, use, disclosure, erasure).
Data Controller	The entity that determines the purposes and means of processing personal data. Rawdah Montessori is the data controller.
Data Processor	A third party that processes personal data on behalf of the data controller (e.g., cloud service providers, payroll providers).
Data Subject	The identified or identifiable person to whom the personal data relates.
Data Protection Officer (DPO)	The designated person responsible for overseeing data protection compliance.
Consent	A freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they signify agreement to the processing of their personal data .
Recognised Legitimate Interest	A new lawful basis introduced by DUAA 2025 for processing necessary for specified public interest purposes, including safeguarding .

5. Key Principles

We adhere to the seven key principles of data protection set out in Article 5 of the UK GDPR:

Principle	Our Commitment
1. Lawfulness, Fairness, and Transparency	We will process personal data lawfully, fairly, and in a transparent manner.
2. Purpose Limitation	We will collect personal data only for specified, explicit, and legitimate purposes and will not further process it in a manner incompatible with those purposes.
3. Data Minimisation	We will collect and process only personal data that is adequate, relevant, and limited to what is necessary for the purposes for which it is processed.
4. Accuracy	We will take reasonable steps to ensure personal data is accurate and, where necessary, kept up to date.
5. Storage Limitation	We will keep personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which it is processed.

Principle	Our Commitment
6. Integrity and Confidentiality (Security)	We will process personal data in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage.
7. Accountability	We will be responsible for, and be able to demonstrate compliance with, the above principles.

6. Lawful Bases for Processing

Under UK GDPR, we must have a valid lawful basis for each processing activity. The most relevant bases for our school are:

Lawful Basis	When We Use It
Consent	For some specific activities where no other lawful basis applies (e.g., consent for photographs, certain direct marketing). Consent must be freely given, specific, informed, and unambiguous. Individuals have the right to withdraw consent at any time .

Lawful Basis	When We Use It
Contract	For processing necessary to fulfil a contract with the individual (e.g., employment contracts with staff).
Legal Obligation	For processing necessary to comply with a legal obligation (e.g., reporting to the DfE, HMRC, or local authority).
Vital Interests	For processing necessary to protect someone's life (e.g., in a medical emergency).
Public Task	For processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority (relevant to some state school functions).
Legitimate Interests	For processing necessary for our legitimate interests (or those of a third party), provided those interests are not overridden by the individual's rights and interests. This is the most appropriate basis for many independent school activities .
Recognised Legitimate Interest	A new basis introduced by DUAA 2025 for processing necessary for certain public interest purposes, including safeguarding. This removes the requirement to carry out a balancing test for these specific purposes .

For **special category data**, we must also identify an additional condition for processing under Article 9 of UK GDPR (e.g., employment, social security, vital interests, or explicit consent) .

7. Special Category Data and Criminal Records Data

We process special category data and criminal records data for specific purposes, including:

- Pupil health information (to support medical needs and safeguarding)
- Staff health information (for occupational health and sickness absence management)
- Religious or philosophical beliefs (as a faith-based school, we process information about faith for admissions and ethos purposes)
- Criminal records data (for safeguarding and safer recruitment checks, in line with our **Safer Recruitment and Criminal Record Disclosure Policy**)

We have established appropriate policies and safeguards for such processing, including:

- Strict access controls
- Enhanced security measures
- Clear retention policies
- Compliance with Schedule 1 of the DPA 2018

8. Roles and Responsibilities

Role	Responsibilities
Governing Body	Overall accountability for data protection compliance; ensuring adequate resources are allocated.
Headteacher	Operational responsibility for implementing this policy; ensuring staff are trained; reporting significant breaches to the Governors.
Data Protection Officer (DPO)	*[Name/Contact]* – Independent oversight of data protection compliance; advice and monitoring; point of contact for the ICO; mandatory role under UK GDPR.
Data Protection Lead (Internal)	*[Name]* – Day-to-day management of data protection; handling subject access requests; maintaining records of processing; staff support.
All Staff	Comply with this policy and associated procedures; complete mandatory training; report any data breaches immediately; handle personal data securely.
ICT Coordinator / Network Manager	Implement and maintain technical security measures; manage user access; support data protection impact assessments for new technologies.

Role	Responsibilities
Greensville Trust (Landlord)	Manages building-wide security systems (CCTV, access control) and the main sign-in system; processes visitor data on behalf of the school under the Service Contract.

9. Data Subject Rights

Individuals have the following rights under UK GDPR:

Right	Description
Right to be Informed	To receive clear and transparent information about how their data is processed (via Privacy Notices).
Right of Access	To obtain confirmation that their data is being processed and access to that data (Subject Access Request) .
Right to Rectification	To have inaccurate personal data corrected.

Right	Description
Right to Erasure (Right to be Forgotten)	To have personal data erased in certain circumstances (e.g., where data is no longer necessary, or consent is withdrawn).
Right to Restrict Processing	To restrict processing in certain circumstances (e.g., while accuracy is contested).
Right to Data Portability	To receive their data in a structured, commonly used format and transmit it to another controller (limited to data processed by consent or contract).
Right to Object	To object to processing based on legitimate interests or public task, or for direct marketing.
Rights Related to Automated Decision-Making	Not to be subject to a decision based solely on automated processing, including profiling, which produces legal or similarly significant effects.

9.1 Subject Access Requests (SARs)

- Requests must be made in writing (a verbal request is valid but we may request written clarification).
- We must respond **within one month**, extendable to three months for complex requests .
- Under DUAA 2025, we are only required to conduct a **reasonable and proportionate search** for information .

- Where a request is for a pupil's educational record, parents have a separate right of access under education regulations. In England, this applies to maintained schools but not independent schools. However, parents may still submit a SAR on behalf of their child if the child is not competent to act on their own behalf .
- We may charge a reasonable fee for repeat requests or for requests that are manifestly unfounded or excessive .
- Information may be withheld if disclosure would likely cause **serious harm** to the physical or mental health of any person, or if it would prejudice safeguarding .

9.2 Requests Involving Children

- Children have the right to make their own SAR if they are competent to do so. The ICO suggests it is reasonable to assume a child has capacity from age 12 .
- Parents may only make a SAR on behalf of their child if the child has authorised them to do so, or if the child lacks capacity.
- Where safeguarding concerns exist, a child's wishes should be considered, but they do not override our duty to protect the child .

10. Data Sharing and Safeguarding

Data protection law is **not a barrier to safeguarding**. The ICO is clear that organisations should not hesitate to share information to prevent harm .

- We will share personal data with relevant agencies (e.g., police, social services, LADO) where necessary to safeguard children or adults at risk.
- Where we regularly share data with other organisations, we will establish **formal data sharing agreements** .
- In emergency situations, we will share information without a formal agreement and **record what was shared, with whom, and why**.
- The DUAA 2025 'recognised legitimate interest' basis supports safeguarding processing without requiring a balancing test .

11. Data Security

We implement appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

11.1 Technical Measures

- Firewalls and antivirus protection
- Encryption of devices and data in transit
- Secure authentication (strong passwords, multi-factor authentication where appropriate)
- Regular security updates and patches
- Restricted access based on role

- Secure Wi-Fi networks

11.2 Organisational Measures

- Clear desk policy
- Secure filing cabinets for paper records
- Staff training on information security
- Data protection impact assessments for new processing activities
- Regular security audits

11.3 Personal Devices

- Staff must not use personal devices to store school data unless encrypted and approved .
- Remote working must follow secure practices.

12. Data Breach Management

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

12.1 Reporting a Breach

Any suspected or actual data breach must be reported **immediately** to:

- The Data Protection Lead
- The Headteacher
- The DPO (for notifiable breaches)

12.2 Investigation and Notification

- We will investigate all breaches promptly.
- Where a breach is likely to result in a risk to individuals' rights and freedoms, we will notify the **ICO within 72 hours**.
- Where a breach is likely to result in a high risk to individuals, we will notify affected individuals without undue delay.
- All breaches will be documented, including facts, effects, and remedial actions taken.

13. Data Retention and Disposal

We retain personal data only for as long as necessary for the purposes for which it was collected, taking into account legal, regulatory, and operational requirements.

- Retention periods are set out in our **Data Retention Schedule** (available on request).
- When data is no longer required, it will be securely disposed of:
    - **Paper records:** Shredded or disposed of via confidential waste
    - **Electronic records:** Permanently deleted using secure deletion software
- Disposal of special category data is subject to enhanced controls.

14. Data Processors and Third Parties

Where we engage third parties to process personal data on our behalf (e.g., cloud providers, payroll services, catering providers), we will:

- Conduct due diligence on their data protection practices.
- Enter into a **written contract** containing UK GDPR-compliant data protection clauses.
- Ensure they process data only on our documented instructions.
- Require them to implement appropriate security measures.
- Monitor their compliance where appropriate.

All third-party contracts must include provisions for data breach notification, data subject rights assistance, and data deletion upon contract termination .

15. International Data Transfers

We will only transfer personal data outside the UK where:

- The destination country has an **adequacy decision** from the UK government; or
- Appropriate **safeguards** are in place (e.g., International Data Transfer Agreement, Binding Corporate Rules); or
- A specific **derogation** applies (e.g., explicit consent, necessary for a contract).

Under DUAA 2025, the threshold for transfers has changed from 'essential equivalence' to protections not being **'materially lower'** than UK standards .

16. Privacy Notices

We provide clear, accessible privacy notices to individuals explaining:

- Who we are and how to contact us
- What data we collect and why
- Our lawful basis for processing

- Who we share data with
- How long we retain data
- Individuals' rights
- How to complain

Separate privacy notices are maintained for:

- Pupils and parents
- Staff
- Website users
- Visitors and contractors

17. Complaints

Under DUAA 2025, we are required to have a formal complaints process for data protection concerns .

17.1 Internal Complaints

If an individual believes their data protection rights have been breached, they should first raise their concern with the **Data Protection Lead** or **Headteacher**.

We will:

- Acknowledge the complaint within **30 days**.
- Investigate promptly and fairly.
- Provide a written outcome.
- Keep the complainant informed of progress.

17.2 ICO Complaints

If the individual is dissatisfied with our response, they may complain to the **Information Commissioner's Office (ICO)** :

- **Website:** www.ico.org.uk
- **Phone:** 0303 123 1113
- **Address:** Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

18. Training and Awareness

- All staff will receive data protection training as part of their induction and annually thereafter.
- Training will cover:
    - Key principles and legal requirements

    - Recognising and handling personal data securely
    - Identifying and reporting data breaches
    - Handling subject access requests
    - Safeguarding and data sharing
- Staff with specific responsibilities (e.g., admissions, HR, ICT) will receive additional targeted training.
- Governors will receive training on their data protection responsibilities.

19. Links with Greensville Trust (Landlord)

As the school occupies premises owned by **Greensville Trust**, the following applies:

- The Trust operates building-wide systems that process personal data, including:
    - **CCTV** covering common parts and external areas
    - **Access control systems** (electronic fobs/cards)
    - The **main building sign-in/out system** for visitors
- The Trust acts as a separate data controller for its own processing activities.
- Where the Trust processes data on our behalf (e.g., visitor data for safeguarding purposes), this is governed by the **Service Contract**, which includes data protection provisions.

- Any data protection concerns relating to Trust-operated systems should be reported to the Headteacher, who will liaise with the Trust.

20. Related Policies

This policy should be read in conjunction with:

- Safeguarding and Child Protection Policy
- Social Media and ICT Policy
- Staff Code of Conduct
- Privacy Notices (various)
- Service Contract with Greensville Trust

21. Monitoring and Review

This policy will be reviewed **annually** by the Headteacher and Governing Body, or sooner following:

- A significant data breach
- Changes in legislation or ICO guidance
- Changes to the school's processing activities

- Recommendations from the ICO or DPO

Review of Policy Dates

REVIEW DATE	REVIEWED BY	SIGNED OFF (Name & Role)
Oct 2025	Governing Body	**Chair:** Sohaib Tanvir
Next Review Due:		
Oct 2026	Governing Body	**Chair:**
	Headteacher	**Headteacher:**