Rawdah Montessori Primary School
Privacy, CCTV and Photography Policy

Version: 2.0
Reviewed: October 2025
Next Review Due: October 2026

1. Introduction

Rawdah Montessori Primary School is committed to protecting the privacy, dignity, and personal data of all pupils, staff, parents, and visitors. As a faith-based independent school, we operate within the framework of Islamic values of respect, integrity, and accountability, and comply fully 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)** .

This policy outlines how personal data, CCTV footage, and photography are collected, used, and stored at Rawdah Montessori Primary School. It should be read in conjunction with the:

- **Data Protection Policy**
- **Safeguarding and Child Protection Policy**
- **Social Media and ICT Policy**
- **Staff Code of Conduct**
- **Service Contract with Greensville Trust** (for shared site CCTV arrangements)

2. Purpose

The purpose of this policy is to:

- Ensure the school meets legal data protection obligations.
- Protect individuals' rights to privacy and confidentiality.
- Provide clarity on the use of CCTV and photography within the school environment.
- Outline consent procedures and safeguarding measures for image and video usage.
- Ensure transparency about how data is collected, used, and shared.

3. Scope

This policy applies to:

- All staff, pupils, parents, governors, contractors, and volunteers.
- All data processed by the school, whether in electronic or paper form.
- All CCTV systems, cameras, and photographic or video recording equipment used on school premises or during school activities.
- Building-wide CCTV systems operated by **Greensville Trust** in common parts of the shared site.

4. Legal Framework

This policy is based on the following legislation and guidance:

Legislation / Guidance	Relevance
UK General Data Protection Regulation (UK GDPR)	The primary regulation governing the processing of personal data.
Data Protection Act 2018 (DPA 2018)	Supplements the UK GDPR and provides exemptions.
Data (Use and Access) Act 2025 (DUAA 2025)	Introduces updates to data protection, including provisions for CCTV and ANPR .
Protection of Freedoms Act 2012	Sets out requirements for CCTV, including signage and codes of practice .
Surveillance Camera Code of Practice (Home Office)	Provides guidance on the appropriate use of surveillance cameras .
Freedom of Information Act 2000	Governs access to information held by public authorities (where applicable).
Education (Independent School Standards) Regulations 2014	Requires independent schools to have arrangements to safeguard and promote the welfare of pupils.
Keeping Children Safe in Education (KCSIE 2025)	Emphasises the importance of safeguarding in all aspects of school life.
Human Rights Act 1998	Protects the right to privacy under Article 8.

5. Data Protection Principles

Rawdah Montessori Primary School ensures that all personal data are:

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.
3. Data Minimisation	We will collect and process only personal data that is adequate, relevant, and limited to what is necessary.
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 for no longer than is necessary for the purposes for which it is processed.
6. Integrity and Confidentiality (Security)	We will process personal data in a manner that ensures appropriate security.
7. Accountability	We will be responsible for, and be able to demonstrate compliance with, the above principles.

6. Data Controller and Data Protection Officer

- **Data Controller:** The Headteacher acts as the Data Controller on behalf of Rawdah Montessori Primary School.
- **Data Protection Officer (DPO):** The school's DPO is responsible for overseeing compliance, advising staff, and responding to data protection requests.

Role	Contact
Headteacher (Data Controller)	*[Name and contact details]*
Data Protection Officer (DPO)	*[Name and contact details]*

7. Personal Data Collection and Use

The school collects and processes personal data such as:

Category	Examples
Pupil Records	Contact details, medical information, academic records, attendance, safeguarding records.
Parent/Guardian Information	Contact details, emergency contacts, fee-payer information.
Staff Information	Employment records, payroll data, qualifications, references, DBS checks.
Financial Information	Fee payment records, bank details, invoicing information.

CCTV Recordings	Footage of individuals on school premises.
Photographs and Videos	Images of pupils and staff for educational, promotional, or archival purposes.

Data are used for legitimate educational and administrative purposes, including:

- Ensuring pupil welfare and safety.
- Communicating with parents.
- Managing school operations and staffing.
- Complying with legal obligations.
- Promoting the school and celebrating achievements.

8. CCTV Usage

8.1 Purpose of CCTV

The school uses Closed-Circuit Television (CCTV) for:

- Ensuring the safety and security of pupils, staff, and visitors.
- Protecting school property and deterring criminal activity.
- Monitoring access points, entrances, and outdoor areas.
- Assisting in the investigation of incidents (e.g., accidents, theft, safeguarding concerns).

The use of CCTV is justified under our **legitimate interests** as a data controller, balanced against the rights and freedoms of individuals .

8.2 Scope of CCTV Coverage

CCTV cameras are operational in specified areas, including:

- Main entrance and reception
- External play areas
- Corridors and communal areas
- Car parks and access roads

Cameras are **not** placed in private areas such as toilets, changing rooms, or classrooms where there is a reasonable expectation of complete privacy.

8.3 Signage

Clear, prominent signs are displayed at all entrances to the school and within camera range, informing individuals that CCTV is in operation. Signs include:

- The purpose of CCTV
- The identity of the data controller
- Contact details for further information

8.4 Legitimate Interest Assessment

The school has conducted a **Legitimate Interest Assessment (LIA)** for its use of CCTV, considering:

- The purpose and necessity of the surveillance.
- The potential impact on individuals' privacy.

- Measures to minimise intrusion.

8.5 CCTV Management

- CCTV operates **24 hours a day, 7 days a week**.
- Recordings are stored securely on password-protected systems with restricted access.
- Access to live and recorded footage is strictly limited to authorised personnel (e.g., Headteacher, DSL, Site Manager, and designated security staff from Greensville Trust).
- Footage is retained for a maximum of **30 days**, unless required for an ongoing investigation or legal proceedings. Where footage is retained longer, the reason is documented.

8.6 Access to Footage

Individuals have the right to request access to CCTV images of themselves under the UK GDPR (Subject Access Request). Requests should be made in writing to the Headteacher or DPO.

- We will respond within **one month**.
- Footage involving other identifiable individuals may be redacted or withheld in accordance with data protection law.
- Where footage is disclosed, it will be provided in a secure format.

8.7 CCTV Operated by Greensville Trust (Landlord)

As the school occupies premises owned by **Greensville Trust**, building-wide CCTV systems covering common parts (e.g., main building entrance, shared corridors, external car parks) are operated by the Trust.

- The Trust acts as a separate **data controller** for its own CCTV processing.

- The Trust has its own CCTV policy and signage.
- The school will liaise with the Trust regarding any requests for footage from these areas.
- Any concerns about Trust-operated CCTV should be reported to the Headteacher, who will escalate to the Trust.

9. Photography and Video Recording

Photographs and video recordings are used to celebrate school life, support learning, document pupil progress, and promote the school's activities, while safeguarding all pupils.

9.1 Consent for Pupil Images

Written parental consent is obtained before taking or using any images of pupils. Consent is sought:

- At the point of admission.
- When there is a significant change in the use of images (e.g., new promotional materials).
- Annually as part of the data collection update.

Parents are asked to specify whether images may be used for:

Use	Description
Internal Use	Classroom displays, learning journals, internal newsletters, school records.

Use	Description
School Website	Images on the school's public website.
Social Media	Images on official school social media accounts (e.g., Facebook, Instagram, X).
Promotional Materials	Brochures, leaflets, advertisements, press releases.
External Media	Local newspapers or publications (rare, and only with explicit consent).

Consent may be withdrawn at any time by notifying the school in writing. Once images have been published (e.g., on social media or in print), it may not be possible to recall them completely.

9.2 Photography by Parents and Carers

- Parents and carers are welcome to take photographs and videos at school events (e.g., sports day, assemblies, concerts) for **personal use only**.
- Images must not be shared on public social media or any public platform without the explicit consent of all parents whose children are identifiable in the image.
- The school reserves the right to restrict photography at specific events for safeguarding or privacy reasons. This will be clearly communicated in advance.

9.3 Photography by Staff

- Staff must only use **school-approved devices** for taking photographs or videos of pupils.

- Images must be stored securely on the school network or approved cloud storage, not on personal devices.
- Staff must not use personal phones or devices to photograph pupils under any circumstances.
- Images must be deleted when no longer needed for the purpose for which they were collected.

9.4 Photography by External Professionals

- Where an external photographer is engaged (e.g., for school photographs), the school will ensure they sign a contract including data protection clauses and are briefed on safeguarding requirements.
- Parents will be informed in advance and given the opportunity to opt out.

9.5 Use on Social Media

- The school may share photos and videos on official platforms only with appropriate consent.
- No image will be published with identifying information such as full names, addresses, or personal details.
- Where group photos are used, individual children will not be named.
- Staff must not share images of pupils on their personal social media.

9.6 Learning Journals and Observations

- Photographs and videos may be taken as part of ongoing observations and assessments (e.g., Montessori record-keeping, learning journals).
- These images are for educational purposes and are stored securely.
- Parents have access to their own child's learning journal but not to images of other children.

10. Data Retention

Type of Data	Retention Period
CCTV Footage	30 days (unless required for investigation)
Photographs and Videos (general)	Retained only while relevant for educational or promotional use; reviewed annually
Learning Journal Images	Retained while child is at the school; transferred to parents on departure
Consent Forms	Retained until consent is withdrawn or child leaves the school
Subject Access Request Records	3 years from completion of request
Data Breach Records	3 years from date of breach

All records are retained and disposed of in line with the school's **Data Retention Schedule** and **Data Protection Policy**.

11. Data Security

- All digital data are stored securely on password-protected systems with restricted access.
- Paper records are stored in locked cabinets.
- Portable devices (e.g., laptops, tablets) are encrypted and used only for legitimate purposes.
- CCTV footage is stored on secure servers with access logs.
- Any data breach will be reported immediately to the DPO and investigated under the school's **Data Breach Procedure**.

12. Rights of Individuals

Under data protection law, individuals have the following rights:

Right	Description
Right to be Informed	To receive clear information about how their data is processed (via this policy and 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 to Erasure	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.

Requests should be made in writing to the Data Protection Officer. We will 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 in response to a Subject Access Request .

13. Data Breach Management

In the event of a data breach, the school will:

1. **Contain and Assess:** Immediately contain the breach and assess its severity.
2. **Notify the ICO:** If the breach is likely to result in a risk to individuals' rights and freedoms, notify the **Information Commissioner's Office (ICO)** within **72 hours** .
3. **Inform Affected Individuals:** If the breach is likely to result in a high risk to individuals, inform them without undue delay.
4. **Record:** Record all breaches in the school's **Data Breach Register**, including facts, effects, and remedial actions.

14. Complaints

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

If dissatisfied with the 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

15. Links with Greensville Trust (Landlord)

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

- The Trust operates building-wide CCTV systems covering common parts (entrances, corridors, car parks). The Trust is a separate data controller for these systems.
- The school will cooperate with the Trust in the event of an investigation requiring CCTV footage.
- Any requests for footage from Trust-operated systems should be made via the Headteacher, who will liaise with the Trust.
- The school's own CCTV systems cover internal school areas and are solely under the school's control.

16. Training and Awareness

- All staff receive training on privacy, CCTV, and photography as part of their induction and annually thereafter.
- Training covers:
    - This policy and its requirements.
    - Consent procedures for photography.
    - Secure handling of images and data.
    - Reporting of breaches or concerns.

- Staff with specific responsibilities (e.g., website management, social media) receive additional guidance.

17. Related Policies

This policy should be read in conjunction with:

- Data Protection Policy
- Safeguarding and Child Protection Policy
- Social Media and ICT Policy
- Staff Code of Conduct
- Acceptable Use Agreements
- Service Contract with Greensville Trust

18. Monitoring and Review

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

- A significant data breach.
- Changes to legislation or ICO guidance (e.g., UK GDPR, DUAA 2025 updates).
- Changes to the school's CCTV or photography practices.
- A recommendation from an external audit or inspection.

Appendix A – Photography Consent Form

Child's Name:

Class:

Date:

Please tick as appropriate:

Use	Consent Given (✓)
Internal displays, classroom use, learning journals	☐
School website	☐
Official school social media accounts	☐
Promotional materials (brochures, leaflets, advertisements)	☐
External media (local newspapers, with prior notice)	☐

I understand that:

- I may withdraw consent at any time by notifying the school in writing.
- Once images have been published, it may not be possible to recall them completely.

- My child will not be identified by name alongside their image on public platforms.
- Images will be stored securely and used only for the purposes I have agreed.

Parent/Carer Signature: _____ Date: _____

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:**