Rawdah Montessori Primary School
Access and Security Policy

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

1. Policy Statement

Rawdah Montessori Primary School is committed to providing a safe and secure environment for all pupils, staff, parents, visitors, and contractors. The school recognises its duty of care under the **Health and Safety at Work etc. Act 1974** and the **Education (Independent School Standards) Regulations 2014** to safeguard all individuals on its premises.

As a faith-based school, our Islamic values of responsibility, care for others, and integrity underpin our commitment to maintaining a secure environment where children can learn and thrive.

The school acknowledges that it occupies premises owned by **Greensville Trust**, and that certain security functions (including building-wide CCTV and the main sign-in system) are provided by the Trust's 24-hour security team. This policy sets out the shared responsibilities between the school and the Trust to ensure a cohesive approach to site security.

This policy should be read in conjunction with the:

- **Safeguarding and Child Protection Policy**
- **Lockdown Procedure Policy**

- **Privacy, CCTV and Photography Policy**
- **Data Protection Policy**
- **Social Media and ICT Policy**
- **Contractor Policy**
- **Service Contract with Greensville Trust**
- **Lone Working Policy**

2. Aims and Scope

The aims of this policy are to:

- Ensure the safety and security of all pupils, staff, and visitors.
- Control access to the school premises effectively.
- Protect against unauthorised entry and potential threats.
- Ensure compliance with all relevant legislation and statutory guidance.
- Establish clear procedures for managing visitors, contractors, and deliveries.
- Provide guidance on responding to security incidents, including intruders.
- Clarify the division of responsibilities between the school and Greensville Trust.

This policy applies to all staff, volunteers, parents, visitors, and contractors at Rawdah Montessori School.

3. Legal Framework

This policy is guided by the following legislation and guidance:

Legislation / Guidance	Relevance
Health and Safety at Work etc. Act 1974	Places a duty on employers to ensure, so far as is reasonably practicable, the health, safety, and welfare of employees and others .
The Management of Health and Safety at Work Regulations 1999	Requires employers to assess risks and implement control measures.
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)	Part Two sets out the safeguarding duties of schools, including site security and visitor management .
Data Protection Act 2018 / UK GDPR	Governs the processing of personal data, including visitor records and CCTV footage.
Equality Act 2010	Requires the school to make reasonable adjustments for disabled visitors and staff.

Legislation / Guidance	Relevance
Protection of Freedoms Act 2012	Sets out requirements for CCTV and surveillance.

4. Roles and Responsibilities

Role	Responsibilities
Headteacher	Overall responsibility for site security; ensuring this policy is implemented and reviewed; making final decisions in security incidents.
Designated Safeguarding Lead (DSL)	Oversee safeguarding aspects of site access; ensure all visitors and contractors are appropriately vetted; lead on safeguarding-related security incidents.
School Administrator / Office Staff	Manage the visitor sign-in system; issue visitor badges; conduct daily security checks; act as first point of contact for visitors.
Site Manager / Facilities Lead	Coordinate with Greensville Trust security team; oversee physical security measures (locks, gates, alarms); conduct regular security audits.

Role	Responsibilities
All Staff	Follow entry and exit procedures; wear identification badges; challenge unknown visitors politely; report any security concerns immediately.
Greensville Trust Security Team	Operate building-wide CCTV systems; monitor the main building entrance; manage the central sign-in system; provide 24-hour security patrols; respond to alarms and incidents .
Visitors and Contractors	Comply with sign-in procedures; wear visitor badges at all times; follow school security instructions.

5. Physical Site Security

5.1 Perimeter and Building Security

- All perimeter gates and external doors remain **locked during the school day**, except during controlled drop-off and collection times.
- Access to classrooms and internal areas is restricted to authorised personnel only.
- Fire exits remain **unlocked but alarmed** to ensure safety and compliance with fire regulations. These doors are for emergency use only and will trigger an alarm if opened.

- The Site Manager or designated staff member conducts **daily visual checks** of gates, locks, fences, and entry systems. Any defects are reported immediately and repaired as a priority.

5.2 CCTV

- CCTV cameras are operational in key areas, including entrances, corridors, external play areas, and car parks.
- CCTV is used for safeguarding and security purposes and is managed in line with the **Privacy, CCTV and Photography Policy**.
- Building-wide CCTV covering common parts is operated by **Greensville Trust**. The school liaises with the Trust for any requests for footage .

5.3 Lighting

- External lighting is maintained around all entrances, car parks, and walkways to deter intruders and ensure safe access during darker hours.
- Any faulty lighting is reported to the Site Manager or Greensville Trust (for building-wide areas) immediately.

6. Access Procedures for Staff

- All staff are issued with an **ID badge** which must be worn visibly at all times while on site.
- Staff use designated entry points and must ensure doors close securely behind them.
- Staff must not hold doors open for unknown individuals or allow tailgating.

- Staff leaving the site outside of normal hours must ensure they have the necessary access fobs/keys and follow lone working procedures.

7. Visitor Management

7.1 Sign-In Procedure

All visitors must:

1. Report to the **main reception** immediately upon arrival.
2. Sign in using the building-wide **electronic sign-in system** operated by Greensville Trust (or a paper visitor log if the system is unavailable).
3. Provide proof of identity (e.g., photo ID) if requested.
4. State the purpose of their visit and whom they are visiting.
5. Read and acknowledge the visitor safeguarding information displayed at reception.
6. Wear a **visitor badge** at all times while on site.

The sign-in system records:

- Full name
- Organisation (if applicable)
- Date and time of arrival
- Person/department being visited
- Time of departure

7.2 Supervision of Visitors

- Visitors (including parents) are expected to be **supervised or accompanied** by a member of staff unless prior authorisation has been given by the Headteacher or DSL.
- Any visitor found unaccompanied or without a valid visitor badge should be **politely challenged** by any member of staff (see Section 7.4).

7.3 Regular Visitors and Volunteers

- Regular visitors (e.g., peripatetic teachers, therapists, volunteers) who have undergone appropriate DBS checks may be issued with a **regular visitor pass** or staff ID badge, at the discretion of the Headteacher.
- Such individuals remain subject to supervision requirements and must sign in and out daily.

7.4 Challenging Unknown Individuals

All staff have a responsibility to maintain site security. If you see an individual you do not recognise who is not wearing a visitor badge:

1. **Approach politely:** "Good morning/afternoon. Can I help you? All visitors are required to sign in at reception."
2. **Escort to reception:** If they are a genuine visitor, escort them to reception to sign in.
3. **Report concerns:** If the individual is unable to provide a valid reason for being on site, or if you feel unsafe, do not challenge further. Immediately:
    - Alert the DSL, Headteacher, or School Administrator.
    - If the individual refuses to leave or poses an immediate threat, **call 999**.

7.5 Refusal of Access

The school reserves the right to refuse access to any individual who:

- Cannot provide a valid reason for visiting.
- Refuses to comply with sign-in procedures.
- Has previously been barred from the premises due to behaviour.
- Is believed to pose a risk to pupils or staff.

8. Contractor and Delivery Management

8.1 Contractors

All contractors must:

- Sign in at reception and present valid identification.
- Provide evidence of a current **enhanced DBS certificate** before commencing work in areas accessible to pupils. If no DBS check is available, the contractor must be **supervised at all times** by a member of school staff .
- Provide risk assessments and method statements (RAMS) for any work that may pose a risk to pupils or staff.
- Wear a **contractor badge** at all times.
- Report to the Site Manager before starting work and on completion.

Contractors are referred to the separate **Contractor Policy** for full details.

8.2 Deliveries

- Deliveries are accepted only at designated times (usually before 9:00 am or after 3:30 pm) and at designated locations.
- Delivery personnel must report to reception and are not permitted to wander unaccompanied.
- Staff receiving deliveries must ensure the delivery area is secure and that pupils are not in the vicinity during the delivery.

---

9. Collection of Children

The safety of pupils during collection is paramount.

- Parents and authorised adults may enter the premises only during allocated drop-off and pick-up times.
- Staff will release children **only to known or authorised adults**.
- If a child is to be collected by someone not known to staff, the parent must:
  - Notify the school in advance (by phone, email, or via the parent app).
  - Provide the name of the authorised person.
  - Where possible, provide a **password** which the authorised person must quote to staff.
- If there is any doubt about the identity of the adult collecting a child, staff must:
  - Politely ask for identification.
  - Verify the collection with the parent (by phone) before releasing the child.
  - If verification is not possible, retain the child in school and contact the Headteacher or DSL immediately.
- **Never release a child to an unauthorised or unknown person.**

10. Security During the School Day

- All external doors remain **locked and secured** during the school day.
- Staff supervise pupils at entry and exit points during drop-off and pick-up.
- Any suspicious person or activity must be reported immediately to the DSL or Headteacher.
- If an intruder refuses to leave the premises, the Headteacher or DSL will contact the police immediately. Do not attempt to physically remove an intruder.

11. Lockdown and Intruder Protocol

In the event of an intruder or serious external threat, the school may implement a **lockdown**. This procedure ensures all pupils and staff are moved to a place of safety and that entry and exit points are secured.

- Staff will be alerted by a distinct alarm signal (**three short bell rings**) or a verbal instruction from the Headteacher or DSL.
- All external and internal doors will be locked.
- Blinds will be closed, lights switched off.
- Pupils will remain quietly seated away from doors and windows.
- The Headteacher or DSL will liaise with the police and emergency services.
- Parents will be notified **only when it is safe to do so**, not during the active incident.

For full details, refer to the separate Lockdown Procedure Policy.

12. Key and Fob Management

- Keys and access fobs are issued only to staff who require them for their role.
- A register of all keys and fobs is maintained by the Site Manager.
- Lost or stolen keys/fobs must be reported **immediately** to the Site Manager and Headteacher.
- Keys and fobs must not be lent to others or left unattended.
- On termination of employment, all keys and fobs must be returned to the School Administrator.

13. Data and Information Security

- Confidential data and school records are stored securely, both physically and digitally.
- Access to data systems is password protected and restricted to authorised personnel only.
- Paper files containing personal data are kept in **locked cabinets**.
- Staff must follow the **Data Protection Policy** and **Social Media and ICT Policy** when handling personal data.
- Visitor logs (electronic or paper) are retained securely and disposed of in line with the school's Data Retention Schedule.

14. Lone Working

- Staff working alone on site (e.g., before or after normal hours) must follow the **Lone Working Policy**.
- Staff should ensure they have a means of communication (e.g., mobile phone) and inform a colleague or family member of their expected finish time.

- External doors must be kept locked, and no unauthorised individuals should be admitted.

15. Training and Awareness

- All staff receive access and security training as part of their induction and annually thereafter.
- Training covers:
    - This policy and its requirements.
    - Visitor sign-in procedures.
    - Challenging unknown individuals.
    - Emergency procedures (including lockdown).
    - Key and fob management.
    - Reporting security concerns.
- The DSL ensures that security awareness is maintained and reinforced through regular briefings and updates.

16. Incident Reporting and Investigation

- Any security incident (e.g., unauthorised entry, suspicious behaviour, lost keys) must be reported immediately to the Headteacher or DSL.
- An incident report will be completed and retained securely.
- Significant incidents will be investigated, and lessons learned will inform updates to this policy.
- Where a crime may have been committed, the police will be informed.

17. Links with Greensville Trust (Landlord)

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

- The Trust operates a **24-hour security team** responsible for:
    - Building-wide CCTV monitoring.
    - The main building entrance sign-in system.
    - Responding to alarms and security incidents.
- The school's Site Manager maintains regular contact with the Trust's security team to coordinate security arrangements.
- Any defects in building-wide security systems (e.g., main entrance door, external lighting, CCTV) should be reported to the Trust via the Site Manager.
- The Trust's security team will support the school in the event of a lockdown or other major security incident.

18. Monitoring and Review

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

- A security incident or breach.
- Changes to legislation or statutory guidance (e.g., KCSIE updates).
- Changes to the school's premises or security systems.
- A recommendation from an external audit or inspection.

The review will include consultation with the DSL, Site Manager, and, where appropriate, Greensville Trust.

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:**