rawdah
MONTESSORI

Rawdah Montessori Primary School

Social Media and ICT Policy

Version: 1.0

Reviewed: October 2025

Next Review Due: October 2026

1. Policy Statement

Rawdah Montessori Primary School recognises the vital role that information and communication technology (ICT) plays in modern education. We are committed to harnessing the benefits of technology to enhance teaching, learning, and communication, while ensuring that all pupils, staff, and the school community are protected from potential risks.

This policy sets out the expectations for the safe, responsible, and professional use of all ICT systems, devices, and social media platforms within the school environment. It applies to all staff, volunteers, governors, and, where appropriate, pupils and visitors.

As a faith-based school, our Islamic values of honesty, integrity, and respect for others underpin our approach to online safety and digital conduct.

This policy should be read in conjunction with the:

- **Safeguarding and Child Protection Policy**
- **Staff Code of Conduct**
- **Data Protection Policy**
- **Acceptable Use Agreements (for staff and pupils)**
- **Whistleblowing Policy**
- **Disciplinary Policy**

2. Purpose and Aims

The purpose of this policy is to:

- Ensure the safe and responsible use of ICT and social media across the school.
- Protect pupils and staff from online harms, including cyberbullying, exploitation, and inappropriate content.
- Maintain professional boundaries between staff, pupils, and parents.
- Safeguard the school's reputation and the integrity of its staff.
- Ensure compliance with all relevant legislation and statutory guidance.
- Provide clear guidance on the consequences of misuse.

3. Legal Framework

This policy is guided by the following legislation and guidance:

Legislation / Guidance	Relevance
Keeping Children Safe in Education (KCSIE 2025)	Sets out safeguarding duties, including online safety and staff-pupil boundaries.
Data Protection Act 2018 / UK GDPR	Governs the processing of personal data and the use of images.
Prevent Duty Guidance	Requires schools to protect pupils from radicalisation and extremist content online.
Copyright, Designs and Patents Act 1988	Protects intellectual property rights.
Communications Act 2003 / Malicious Communications Act 1988	Covers offensive or threatening electronic communications.
Protection from Harassment Act 1997	May apply to online harassment or cyberbullying.

Legislation / Guidance	Relevance
Education Act 2011	Gives schools powers to search for and delete electronic content.
Equality Act 2010	Protects against online discrimination or harassment related to protected characteristics.

4. Scope

This policy applies to:

- All staff (teaching, support, administrative, and leadership)
- Volunteers and governors
- Pupils (where referenced in specific sections)
- Contractors and agency staff working on school premises
- Anyone accessing the school's ICT systems or representing the school online

It covers:

- School-owned devices and networks

- Personal devices used on school premises
- Official school social media accounts
- Personal use of social media that may impact the school or professional standing

5. Roles and Responsibilities

Role	Responsibilities
Governing Body	Ensure the school has effective online safety policies and procedures; monitor their implementation.
Headteacher	Overall responsibility for ICT safety and staff conduct; ensure staff are trained; investigate breaches.
Designated Safeguarding Lead (DSL)	Lead on online safety concerns; manage safeguarding incidents related to ICT or social media.
ICT Coordinator / Network Manager	*[Name]* – Manage technical security; filter and monitor content; maintain systems.

Role	Responsibilities
All Staff	Use ICT systems responsibly; model positive online behaviour; report concerns immediately.
Pupils and Parents	Follow Acceptable Use Agreements; report any online safety concerns.
Greensville Trust (Landlord)	Maintain the building's wider network infrastructure and security systems (CCTV, access control).

6. Acceptable Use of ICT

6.1 School-Owned Devices and Networks

- School ICT systems and devices are provided for educational and professional purposes.
- Staff must not expect privacy when using school systems; the school reserves the right to monitor usage in line with its monitoring policy (see Section 11).
- Staff must log off or lock devices when not in use.
- Passwords must be strong, kept confidential, and changed regularly.
- Software and applications may only be installed with authorisation from the ICT Coordinator.

6.2 Personal Devices

- Staff may use personal devices on school premises but must adhere to the following:
  - Personal devices must not be used to take photographs or videos of pupils.
  - Personal devices must not be used to store or access school data, unless via secure, approved systems (e.g., school email via app).
  - Personal devices should be kept secure and out of sight during teaching hours.
  - Staff must not use personal devices to contact pupils or parents, except in emergencies and with prior agreement.

6.3 Internet Access

- Internet access is filtered and monitored to protect users from inappropriate content.
- Staff must not attempt to bypass filtering systems.
- Any accidental access to inappropriate content must be reported immediately to the DSL.

7. Social Media – Professional Use

7.1 Official School Social Media Accounts

- The school may maintain official social media accounts (e.g., Facebook, X/Twitter, Instagram) to celebrate achievements and communicate with parents.
- Only designated staff may post on official accounts.
- Content must be professional, positive, and respectful.
- Parental consent must be obtained before images of pupils are published online (see Section 8).

7.2 Staff Use of Social Media – Personal Accounts

Staff must maintain a clear separation between their professional role and personal online presence.

Staff must not:

- Accept current or former pupils as friends or followers on personal social media accounts.
- Communicate with pupils through personal social media, messaging apps, or gaming platforms.
- Discuss school matters, pupils, parents, or colleagues on personal social media.
- Post anything that could bring the school into disrepute or compromise their professional standing.
- Identify themselves as a staff member of the school on personal accounts where content could be inappropriate.

Staff should:

- Review privacy settings regularly to ensure personal content is not publicly visible.
- Be aware that their online conduct, even on private accounts, may be subject to scrutiny and could be considered in disciplinary proceedings.

8. Photographs and Videos

- Photographs and videos of pupils may only be taken using **school-owned devices**.
- Written parental consent must be obtained before images are taken or published.
- Images must be stored securely and used only for agreed purposes (e.g., learning journeys, school website, official social media).
- Staff must not upload images of pupils to personal devices, personal cloud storage, or personal social media.
- Pupils' full names should not normally be published alongside images on public platforms.
- Any breaches of this policy regarding images will be treated as a safeguarding and disciplinary matter.

9. Communication with Pupils and Parents

9.1 Communication with Pupils

- Staff must not communicate with pupils through personal mobile phones, personal email, or personal social media.
- If communication outside school hours is necessary (e.g., for a school trip), it must be done through official school channels (e.g., school email) and with the knowledge of a parent/carer and the DSL.

9.2 Communication with Parents

- Communication with parents should be professional and conducted through official channels (e.g., school email, parent communication apps, telephone).
- Staff must not share personal contact details with parents.
- If a parent makes inappropriate contact via personal channels, staff should report this to the Headteacher immediately.

10. Data Protection and Cyber Security

- All staff must comply with the **Data Protection Policy** when handling personal data.
- Personal or sensitive data must not be stored on personal devices unless encrypted and approved.
- Emails containing personal data should be sent securely.
- Staff must be vigilant against phishing emails and cyber threats. Any suspicious activity must be reported to the ICT Coordinator.
- Data breaches must be reported immediately to the Headteacher and Data Protection Officer (DPO).

11. Monitoring of ICT Systems

The school reserves the right to monitor its ICT systems to:

- Ensure compliance with this policy.
- Protect the security of the network.
- Investigate suspected misuse.
- Safeguard pupils and staff.

Monitoring may include:

- Review of internet browsing history.
- Review of email communications (where there is a legitimate concern).
- Use of filtering and monitoring software.

Staff will be notified of any monitoring through this policy and induction training.

12. Misuse and Sanctions

Any breach of this policy will be taken seriously and may result in:

- Informal discussion or guidance.
- Formal disciplinary action, up to and including dismissal.
- Referral to the police or other agencies (e.g., for illegal content or activity).
- Referral to the Disclosure and Barring Service (DBS) or Teaching Regulation Agency (TRA) where appropriate.

Examples of misuse include, but are not limited to:

- Accessing or sharing inappropriate or illegal content.
- Cyberbullying or online harassment.
- Breaching pupil or staff confidentiality.
- Using social media to bring the school into disrepute.
- Failing to report a safeguarding concern related to online activity.

13. Online Safety Incidents – Reporting Procedure

Any online safety incident or concern must be reported immediately to the **Designated Safeguarding Lead (DSL)** .

Incident Type	Action
Suspected illegal content or activity	Report to DSL immediately. DSL will liaise with police and/or other agencies.
Cyberbullying (pupil or staff)	Report to DSL or Headteacher. Investigate and take appropriate action under relevant policies.
Accidental access to inappropriate content	Report to DSL. Clear browser history. No further action if genuinely accidental.
Staff-pupil inappropriate online contact	Report to Headteacher immediately. May lead to suspension pending investigation.

14. Training and Awareness

- All staff will receive online safety training as part of their induction and annually thereafter.
- Training will cover:
  - This policy and its requirements.
  - Recognising and reporting online safety concerns.
  - Professional boundaries online.
  - Data protection and cyber security.
- Pupils will receive age-appropriate online safety education as part of the curriculum.
- Parents will be provided with guidance on keeping children safe online.

15. Links with the Landlord (Greensville Trust)

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

- The building's wider ICT infrastructure, including network connectivity and security systems (CCTV, access control), is managed by the Trust.
- Any concerns regarding building-wide systems (e.g., network outages, CCTV access) should be reported to the Headteacher, who will liaise with the Trust's security team.
- The Trust's 24-hour security team operates the main building sign-in/out system, which captures visitor data. This is managed in line with data protection requirements (see Service Contract Clause 4.7).

16. Related Policies

This policy should be read in conjunction with:

- Safeguarding and Child Protection Policy
- Staff Code of Conduct
- Data Protection Policy
- Acceptable Use Agreements (Staff and Pupils)
- Disciplinary Policy

- Whistleblowing Policy
- Anti-Bullying and Harassment Policy

17. Monitoring and Review

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

- A significant online safety incident.
- Changes in legislation or statutory guidance (e.g., KCSIE updates).
- Changes to the school's ICT infrastructure.

Staff Acknowledgment

All staff are required to read this policy and sign the acknowledgment below. The signed form will be kept in the staff member's personnel file.

I confirm that I have read, understood, and agree to abide by the **Rawdah Montessori Primary School Social Media and ICT Policy**.

Name:

Role:

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:**