Visitors Policy
2025-2027

Rida Girls and Rida Boys High School

Paradise Rida Schools Trust

Approved by:	Governors	**Date:** Sep 2025
Last reviewed on:	Sep 2025	
Next review due by:	Sep 2026	

1. Introduction

This policy has been reviewed and updated to reflect:

- **Keeping Children Safe in Education (DfE 2025)** – effective 1 September 2025.
- **DfE Mobile Phones in Schools Guidance (Feb 2024).**
- **DfE Cyber Security Standards for Schools and Colleges (2024).**
- **UK Safer Internet Centre Filtering and Monitoring Guidance (2023).**
- **Online Safety Act 2023 (Ofcom regulatory framework).**
- **Teaching Online Safety in Schools (DfE).**

The policy applies to the whole school community including staff, pupils, governors, parents/carers, third-party suppliers, and contractors.

3. Aims

- Safeguard pupils when using technology.
- Ensure staff, pupils and parents understand online safety responsibilities.
- Establish clear expectations regarding acceptable and unacceptable use of technologies.
- Align with statutory safeguarding and cyber security requirements.

4. Roles and Responsibilities

- **Governing Body/SLT:** Ensure compliance with KCSIE 2025; review filtering & monitoring annually; receive an annual safeguarding and cyber security assurance report.
- **Designated Safeguarding Lead (DSL):** Lead responsibility for online safety; ensure staff training covers current risks including misinformation, disinformation, conspiracy theories, harmful online communities, grooming and radicalisation.
- **All Staff:** Read Part 1 of KCSIE 2025; follow safeguarding procedures; model safe use of technology.
- **IT Manager/MSP:** Maintain compliance with DfE Cyber Security Standards (MFA, patching, backups, access control, asset register, annual cyber audit).

5. Learning and Teaching

The school will deliver online safety education as part of RSHE/PSHE curriculum including: - Safe use of the internet and digital communication. - Understanding and identifying misinformation, disinformation, and conspiracy theories. - Recognising online grooming,

radicalisation, cyberbullying, and sexual exploitation. - Harms from pornography, sexualised content, and online communities promoting self-harm or extremism. - Safe, ethical, and responsible use of generative AI tools. - Financial harms: scams, in-game purchases, gambling risks.

6. Technical Controls

- Filtering and monitoring systems in place, regularly reviewed for effectiveness, with a published annual statement.
- Filtering and monitoring proportionate to risk, reviewed via UK Safer Internet Centre standards.
- Multi-factor authentication (MFA) for staff with privileged access.
- Devices updated with security patches monthly.
- Encrypted and regularly tested backups.
- Secure configuration of cloud services, with Data Processing Agreements from suppliers.

7. Mobile Phones & Devices

- Pupils are prohibited from using personal mobile phones and internet-enabled devices during the school day (including breaks and lunchtimes).
- Exceptions may be made for SEND, medical, or safeguarding reasons, agreed in advance.
- Phones must be left at home, handed in on arrival, or switched off and stored securely.
- Staff must not contact pupils using personal devices.
- Confiscation of devices is permitted under behaviour and disciplinary procedures.

8. Remote Education

- Only school-approved platforms may be used.
- Staff and pupils must use school accounts.
- One-to-one sessions require parental/SLT awareness.
- All participants must be informed if a session is recorded; recordings stored securely.
- Neutral camera backgrounds and professional conduct required.

9. Incident Management

- All safeguarding concerns must follow DSL procedures as per KCSIE 2025.
- Cyber security incidents escalated to IT manager/MSP and reported to DfE/NCSC if required.
- All incidents logged and reviewed for learning.

10. Data Protection & Privacy

- Compliant with Data Protection Act 2018 and UK GDPR.
- Secure handling of personal data, encrypted storage and transmission.
- Use of encrypted USBs and secure remote access.
- Disposal of data/equipment must follow ICO and school policy.

11. Policy Communication

- Policy available on the school website and staff intranet.
- Training for staff at induction and annually.
- Parents informed via newsletters, website, and parent evenings.

12. Monitoring & Review

- DSL to lead an **annual online safety risk assessment**.
- Governors receive annual assurance report covering online safety and cyber security.
- Policy reviewed annually or sooner if guidance changes.