



TRRS ONLINE SAFETY POLICY

INTRODUCTION

At The Roman Ridge School (TRRS), we recognise that technology is a vital driver of academic growth, collaboration, and global citizenship in a modern educational programme. However, digital progress must be balanced with meticulous care for our pupils' safety, mental well-being, and digital integrity.

This policy sets out our approach to online safety - through collaborative leadership, continuous professional development for our teachers and proactive pastoral care, TRRS ensures a digital environment where every child feels secure, valued, and empowered to excel.

This policy forms an integral part of the school's pastoral care and safeguarding apparatus and complies with Data Protection Act (Ghana, 2012) and local regulatory standards governing child protection online, Keeping Children Safe in Education (KCSIE) 2026 (UK Standards for Schools and International Contexts and Standards for British Schools Overseas). It should be read alongside the TRRS Child Protection & Safeguarding Policy.

ROLES AND RESPONSIBILITIES

Instructional leadership requires clear accountability, transparent roles, and empowering staff to act swiftly and decisively.

The Principal, Management & Academic Board of Governors

- Maintain ultimate oversight of safeguarding strategies, ensuring appropriate filtering, monitoring, and infrastructure investments are made annually.
- Conduct an annual review of online safety procedures alongside local risk assessments.

Designated Safeguarding Lead (DSL) & Online Safety Lead

- Take primary responsibility for triage, recording, and actioning all online safety concerns.
- Ensure all safeguarding records regarding digital incidents are securely stored and monitored for trend analysis.
- Deliver regular, context-rich training for staff, aligning international best practices with local classroom realities.

Teaching Staff

- Act as primary caregivers by actively monitoring student behaviour online, whether during ICT lessons, research projects, or extracurricular competitions.
- Embed digital literacy, cyber-ethics, and critical evaluation skills across all key stages.
- Model professional digital boundaries at all times, adhering strictly to the staff code of conduct.

Technical & ICT Department

- Maintain robust perimeter security, content filtering, and active monitoring software across the TRRS network.
- Ensure prompt isolation and reporting of any compromised device or security breach to the Safeguarding Team/Management.

CORE SAFEGUARDING MECHANISMS & INFRASTRUCTURE

Campus Device & Network Infrastructure Rules

To ensure pupil safety, remove digital distractions, and maintain total control over internet traffic, TRRS operates under strict device and network boundaries:

1. Mobile Phone Policy:
 - Pupils are strictly prohibited from bringing or using mobile phones, laptops, tablets, smartwatches or devices that connect to the internet on campus.
 - Any unauthorized device brought onto school grounds will be confiscated immediately in accordance with the Student Code of Conduct and Behaviour Policy.
2. Network Connection Restrictions (No Personal Devices):
 - Neither pupils nor staff are permitted to connect personal devices (laptops, tablets, personal phones, or smartwatches) to the school's network.
 - Only official, school-owned machines are permitted access to the TRRS network infrastructure.

Filtering and Active Monitoring

TRRS implements an integrated digital safety boundary designed to protect without stifling enquiry-led learning:

- Appropriate Filtering: Access to content depicting extreme violence, adult material, illegal activities, radicalisation, and harmful social media challenges is automatically blocked on school networks.
- Proactive Monitoring: Network logs are routinely audited. Check for keywords or search behaviours linked to self-harm, cyberbullying, or inappropriate contact, initiating immediate review by the Safeguarding Team.

Restricted & Monitored Pupil Internet Access:

- Pupil internet access is strictly restricted, monitored, and only accessible to pupils via official IT Laboratories under direct teacher supervision.
- Classroom laptops or tablets assigned to Form Tutors are strictly password-protected and are not accessible to students under any circumstances.
- Wireless access keys/passwords are changed regularly by IT Technicians to make it difficult for students/staff to gain unauthorised access
- Student iPads are checked regularly for unauthorised access and material on the devices
- Staff laptops are also checked regularly by IT maintenance team to ensure full user compliance

EDUCATIONAL INTEGRATION & PUPIL EMPOWERMENT

Online safety is actively integrated into our PSHE, Computing, and Assembly programmes. We partner with reputable organisations and government agencies (KPMG, Cybersecurity Authority) to hold special talks and programmes to sensitise our staff and students about online risks and safe use. Our goal is to cultivate a strong awareness in our pupils, enabling them to navigate digital spaces responsibly. Key curriculum strands include:

1. Digital Footprint & Reputation: Understanding the permanence of online content.
2. Critical Media Evaluation: Differentiating authentic sources from misinformation and online manipulation.
3. Peer Conduct & Respect: Applying our school values—*Responsibility, Integrity, and Morality*—to online interactions, social platforms, and group communications.

PREVENTING & MANAGING ONLINE RISKS

KCSIE 2026 categorizes online risks into **4 Cs** and TRRS addresses each through defined measures:

Risk Category	Definition & Examples	TRRS Safeguarding & Mitigation Strategy
Content	Exposure to illegal, inappropriate, or harmful material (e.g., violence, adult content, misinformation).	Strict firewall filtering, curated digital libraries, and supervised internet access during academic activities.
Contact	Interactions with unknown adults or peers leading to grooming, exploitation, or harassment.	Blocked access to unvetted chat rooms/apps on school networks; education on privacy settings and stranger awareness.

Conduct	Personal behaviour that causes harm (e.g., cyberbullying, sharing illicit images, online harassment).	Clear anti-bullying protocols, restorative pastoral interventions, and strict enforcement of the Student Code of Conduct.
Commerce	Financial exploitation, phishing, unauthorized purchases, or exposure to online gambling.	Restricted administrative rights on pupil devices, disabled in-app purchases on school units, and financial safety lessons in ICT.

INCIDENT RESPONSE & REPORTING PROTOCOL

When an online safety issue arises, staff follow a deliberate, step-by-step response designed to prioritize child safety and emotional well-being:

Step 1: Secure & Ensure Immediate Safety: If a pupil is in distress or exposed to immediate harm, isolate the pupil/device securely. Do not delete evidence.

Step 2: Document & Report: Record facts immediately (date, time, platform, nature of content). Submit Safeguarding Incident Form to Management/Safeguarding Team within 24 hrs.

Step 3: Triage & Assessment: Safeguarding Team/Management evaluates the severity against thresholds. Teacher/Form Tutor provide pastoral care and emotional support to affected children.

Step 4: Parent Engagement & Resolution: Engage Parent/Guardian early through direct, supportive dialogue. Implement restorative sanctions or disciplinary escalation where necessary.

Staff should never attempt to investigate serious allegations involving illegal material independently. Preserve digital evidence (take screenshots, keep URLs) and escalate to Management/Safeguarding Team immediately.

PROFESSIONAL BOUNDARIES & DIGITAL COMMUNICATION

To preserve professional integrity and pupil welfare:

- Staff must not engage with current TRRS pupils via personal social media accounts (Instagram, Snapchat, Tiktok, Discord), messaging apps (Telegram) or personal email addresses.
- All digital communications between staff, pupils, and parents must occur through official TRRS domain emails and approved learning management platforms - MS 365 Outlook or Teams.
- Staff photography or recording of pupils must only occur using school-owned camera equipment (not personal mobile phones or devices) for official educational, news, or celebratory communications approved by Management