

SRI PL***

Online Safety

Implementation Date	May 2025
Last Reviewed	July 2026
Reviewed by	Frances Powell
Scheduled Review Date	July 2027



GEMS
SCHOOL OF
RESEARCH &
INNOVATION

Table of Contents

1. Policy Statement	3
2. Beliefs	3
3. Scope	3
4. Key Online Risks	3
Content Risks.....	4
Contact Risks	4
Conduct Risks	4
Commercial Risks	4
5. Student Expectations	4
6. Staff Responsibilities.....	4
7. Parent Partnership.....	5
8. Digital Citizenship	5
9. Social Media	5
10. Device and Network Use.....	6
11. Artificial Intelligence.....	6
12. Online Bullying and Harassment.....	6
13. Reporting Concerns	7
14. Monitoring and Safeguarding.....	7
15. Data Protection and Privacy	8
16. Education and Awareness.....	8
17. Compliance.....	8
18. Policy Review	8

1. Policy Statement

At GEMS School of Research and Innovation (SRI), technology is an integral part of learning, communication and creativity. We are committed to creating a safe, inclusive and positive digital environment where students can benefit from technology while understanding the responsibilities that accompany its use.

The school recognises that digital technologies present significant opportunities for collaboration, innovation and personal growth. At the same time, students may encounter risks associated with online content, communication, information sharing and emerging technologies. Through education, safeguarding practices and partnership with families, SRI aims to equip students with the knowledge, skills and judgement needed to navigate the digital world safely and responsibly.

2. Beliefs

At SRI, we believe that digital literacy and online safety are essential life skills that support student wellbeing, academic success and responsible citizenship.

We believe that:

- Students should be empowered to use technology confidently, responsibly and ethically
- Online safety is a shared responsibility between students, families, staff and the wider school community.
- Digital wellbeing is as important as physical and emotional wellbeing
- Students should be taught to think critically about information they encounter online and make informed decisions about digital content.
- Respect, kindness and integrity should guide all online interactions.
- Technology should enhance learning while maintaining a healthy balance between online and offline experiences.

3. Scope

This policy applies to:

- All students.
 - All employees.
 - Contractors, consultants and volunteers.
 - Parents and carers when interacting with school digital platforms.
 - School-owned devices, systems and networks.
 - Personal devices used on school premises or for school-related activities.
- Text here

4. Key Online Risks

SRI recognises four broad categories of digital risk:

Content Risks

Exposure to harmful, inappropriate, misleading or age-inappropriate material. This may include violent content, misinformation, extremist material, hate speech, scams or other unsuitable content

Contact Risks

Risks arising from online interaction with others, including strangers, grooming, manipulation, exploitation, harassment or unwanted communication.

Conduct Risks

Behaviour online that causes harm to oneself or others, including cyberbullying, inappropriate sharing of images, misuse of social media and harmful digital behaviour.

Commercial Risks

Risks associated with online advertising, phishing, fraud, scams, gambling, unauthorised purchases and misuse of personal information.

5. Student Expectations

Students are expected to:

- Use digital technology respectfully and responsibly.
- Protect their passwords and account credentials.
- Keep personal information private.
- Use school systems for educational purposes.
- Communicate respectfully online.
- Respect copyright, intellectual property and academic honesty.
- Report concerns, inappropriate content or unsafe behaviour promptly.
- Use Artificial Intelligence tools ethically and in accordance with school expectations.
- Consider the impact of their digital actions on themselves and others.

6. Staff Responsibilities

All staff are expected to:

- Model safe and responsible digital behaviour.
- Promote positive digital citizenship.
- Deliver age-appropriate online safety education.
- Monitor technology use during lessons and school activities.

- Report safeguarding concerns through established safeguarding procedures.
- Maintain appropriate professional boundaries online.
- Protect confidential information and student data.
- Stay informed about emerging technologies and online risks

7. Parent Partnership

Parents and carers play an important role in supporting safe technology use beyond the school environment

The school encourages parents to:

- Maintain open conversations about online activity.
- Monitor age-appropriate use of apps, social media and gaming platforms.
- Establish appropriate screen-time routines.
- Enable privacy and safety settings on devices.
- Discuss respectful online conduct and digital footprints.
- Report concerns to the school where they may impact student wellbeing or safety

8. Digital Citizenship

SRI promotes responsible digital citizenship through the following principles:

- Respect for others online and offline.
- Responsible communication and collaboration.
- Ethical use of information and technology.
- Awareness of personal digital footprints.
- Respect for privacy and consent.
- Safe participation in digital communities.
- Responsible and transparent use of Artificial Intelligence technologies

9. Social Media

Students should:

- Use social media in a respectful and age-appropriate manner.
- Avoid sharing personal or sensitive information publicly.
- Obtain consent before sharing images, videos or information relating to others.
- Report inappropriate messages, content or interactions.

- Understand that online actions may have long-term consequences for reputation and wellbeing.

Where student behaviour on social media affects the safety, wellbeing or reputation of members of the school community, the school reserves the right to investigate and take appropriate action.

10. Device and Network Use

The school's digital infrastructure is designed to support teaching and learning while maintaining appropriate safeguards.

The school will:

- Maintain filtering and monitoring systems.
- Use secure networks and security controls.
- Review digital safety measures regularly.
- Evaluate emerging technologies prior to implementation.
- Promote secure authentication practices.

Students must not:

- Attempt to bypass security systems.
- Access another user's account.
- Use VPNs or other methods to circumvent school restrictions.
- Deliberately access inappropriate material.
- Install unauthorised software or applications.

11. Artificial Intelligence

SRI recognises the growing role of Artificial Intelligence in education.

Students and staff should:

- Use AI tools responsibly and ethically.
- Verify information generated by AI systems.
- Avoid sharing confidential or personal information with AI platforms unless authorised.
- Acknowledge AI use where required by academic expectations.
- Understand that AI-generated content may contain inaccuracies, bias or incomplete information.

12. Online Bullying and Harassment

SRI does not tolerate cyberbullying, online harassment, discrimination, intimidation or harmful online conduct.

Reports of online bullying will be investigated in line with the school's safeguarding and behaviour procedures.

Students are encouraged to:

- Avoid responding to abusive content.
- Save evidence where appropriate.
- Block and report offending users.
- Seek support from a trusted adult or member of staff

13. Reporting Concerns

Students, parents and staff should report any concerns relating to:

- Inappropriate content.
- Online harassment or bullying.
- Suspicious communication.
- Digital safeguarding concerns.
- Misuse of school technology.
- Data security concerns.
- Potential illegal online activity.

Concerns should be reported immediately to:

- A teacher.
- Head of Year or Phase Leader.
- Designated Safeguarding Lead (DSL).
- Information Technology Team, where appropriate.

14. Monitoring and Safeguarding

To safeguard students and maintain security, the school may:

- Monitor activity on school-owned devices and networks.
- Investigate concerns relating to student safety.
- Restrict or suspend access to school digital resources where necessary.
- Review activity logs in accordance with safeguarding and data protection requirements
- Users should not expect complete privacy when using school-managed systems and devices.

15. Data Protection and Privacy

SRI is committed to protecting personal information and managing data responsibly.

All members of the school community are expected to:

- Protect personal and confidential information.
- Use secure passwords.
- Follow school data protection procedures.
- Report suspected data breaches immediately.
- Handle information responsibly and professionally.

16. Education and Awareness

Online safety education is embedded throughout the curriculum and pastoral programme.

Students will receive age-appropriate learning covering:

- Digital citizenship.
- Cybersecurity.
- Privacy and personal information.
- Online relationships.
- Reputation management.
- Misinformation and critical evaluation of information.
- Artificial Intelligence.
- Healthy technology use and digital wellbeing.
- Cyberbullying and online behaviour.

17. Compliance

Failure to comply with this policy may result in:

- Educational intervention.
- Temporary or permanent restriction of technology access.
- Behaviour sanctions.
- Safeguarding action.
- Referral to external authorities where required by law

18. Policy Review

This policy will be reviewed annually or sooner where required by changes in legislation, technology, safeguarding guidance or organisational requirements.