ONLINE SAFETY POLICY

Reviewed:	July 2026
Next Review Due:	July 2027
Applies To:	7Hills Community
Owner:	Head of School
Approved By:	Board of Directors

Mission, Vision and Values

Mission
To inspire our children to reach their full potential by fostering curiosity and an interest in learning, awakening their minds and illuminating their world.

Vision
To create an affordable international secondary school with a high standard of education where children learn through practical and project-based work. To develop our students' moral and intellectual capacity, and to encourage creativity and adaptability.

Aim
An education that is broad, balanced and challenging, with an emphasis on developing strong connections to our host country, Uganda.

Values
Desire for lifelong learning; an ability to adapt; be innovative and reflective thinkers; open minded, and empathetic while achieving high academic success according to individual potential.

Contents

1. Policy Statement and Purpose

2. Scope

3. Guiding Principles

4. Roles & Responsibilities

    4.1 Board of Directors

    4.2 Head of School

    4.3 Designated Safeguarding Lead (DSL)

    4.4 IT Officer

    4.5 All Staff

    4.6 Students

    4.7 Parents and Carers

5. Education, Curriculum and Pastoral Provision

6. Acceptable Use, Professional Conduct and Staff Behaviour

    6.1 Roles and Responsibilities Summary

7. Technical Safeguards: Filtering and Monitoring

8. Use of Personal Devices, Mobile Phones and BYOD

9. Remote Learning, Online Platforms and Digital Communication

10. Responding to Online Safety Incidents

11. Training, Awareness and Professional Development

12. Data Protection, Privacy and Record-Keeping

13.Use of Artificial Intelligence (AI)

14. Audit, Monitoring and Review

1. Policy Statement and Purpose

7Hills International School (7Hills), is committed to safeguarding students and promoting their wellbeing in all aspects of school life, including their engagement with digital technologies and online environments. Online safety is recognised as a safeguarding priority, a curriculum responsibility and a shared community duty.

This policy sets out how the school:

- protects students from online harm, exploitation, bullying and abuse
- promotes responsible, respectful and ethical use of technology
- supports students to develop digital resilience, critical thinking and safe behaviours
- ensures systems, filters and monitoring arrangements reduce risk
- establishes clear expectations for staff conduct and professional use of technology
- provides structured response procedures for incidents and concerns.

The policy aligns with child protection and safeguarding procedures, behaviour expectations, ICT acceptable use agreements and data protection requirements. Online safety is understood not as a stand-alone initiative, but as an integral element of pastoral care, teaching and learning, and whole-school safeguarding culture.

2. Scope

This policy applies to the use of:

- school networks, devices, platforms and digital services
- personal devices used on school premises or for school activities
- school-related online activity, communication and content
- off-site and remote learning environments where school involvement exists.

It covers students, teaching and non-teaching staff, contractors, volunteers, external providers, guest speakers and visitors, as well as expectations of parents and carers as partners in supporting safe and responsible technology use.

3. Guiding Principles

Online safety at 7Hills is guided by the following principles:

- safeguarding comes before convenience or technological preference
- prevention, education and early intervention are prioritised
- students are supported to become responsible, reflective and resilient digital citizens
- harmful behaviours online are treated with the same seriousness as offline conduct
- responses to incidents are proportionate, trauma-informed and centred on student wellbeing
- decision-making is evidence-based and aligned with professional standards and legal expectations.

The school recognises that technology continually evolves. Practice therefore focuses not only on rules and controls, but on building judgement, awareness and ethical understanding.

4. Roles & Responsibilities

4.1 Board of Directors
The Board ensures:

- The policy meets safeguarding expectations and international best practice standards.
- Filtering and monitoring systems are in place and reviewed annually.
- Online safety is embedded in whole-school safeguarding.
- Training for senior leaders and the DSL remains up to date.

4.2 Head of School
Responsible for ensuring:

- Online safety is integrated into policies, curriculum and communication.
- Staff receive regular training on digital safeguarding.
- The DSL has time and resources to lead online safety.
- Parents are educated about digital risks and online behaviours.

4.3 Designated Safeguarding Lead (DSL)
The DSL leads online safety and:

- Monitors, analyses, and responds to online safety incidents.
- Liaises with ICT support, section heads, SENCO and leadership.
- Maintains clear reporting procedures.
- Ensures filtering and monitoring expectations are understood.
- Provides trend analysis and termly updates to the Head and Board.

4.4 IT Officer
Responsible for:

- Maintaining filtering, monitoring, and network security.
- Ensuring software updates, content control, and cyber-security.
- Supporting the DSL during investigations.

4.5 All Staff
All staff must:

- Model safe and responsible online behaviour.
- Follow all Acceptable Use Agreements.
- Report concerns immediately.
- Supervise student use of technology appropriately.
- Teach online safety themes where relevant to their subject.

4.6 Students
Students must:

- Follow the Student Acceptable Use Agreement.
- Report concerns to a trusted adult.
- Use school devices and platforms responsibly.

4.7 Parents and Carers

Parents and carers are expected to:

- Support the school's online safety expectations.
- Engage with guidance provided by the school.
- Inform the school of concerns relating to online activity.

6.8 Roles and Responsibilities Summary

Role	Key Responsibilities
Board of Directors	Strategic oversight, policy approval, assurance
Head of School	Executive accountability, escalation
DSL	Safeguarding response, incident management
IT Officer	Technical controls, monitoring systems
Staff	Supervision, reporting concerns
Students	Responsible use, reporting issues
Parents	Support adherence to guidelines, report concerns

5. Education, Curriculum and Pastoral Provision

Online safety is reinforced through pastoral programmes, PSHE, subject learning and assemblies, with age-appropriate emphasis on areas such as:

- respectful communication and digital citizenship
- cyber-bullying and peer conflict online
- privacy, consent, sharing of images and digital reputation
- misinformation, manipulation and online influence
- wellbeing, screen time balance and help-seeking behaviour.

Where appropriate, teaching also addresses higher-risk themes sensitively and developmentally, including exposure to harmful content, grooming risks and harmful sexual behaviour in digital contexts. Students are encouraged to think critically rather than being given only prohibitive rules.

6. Acceptable Use, Professional Conduct and Staff Behaviour

All staff must adhere to the school's acceptable use expectations, including:

- maintaining clear professional boundaries online
- not contacting students via personal accounts or platforms
- using school communication channels for school business
- ensuring privacy, confidentiality and safeguarding considerations guide decisions.

Breaches of professional conduct online may be managed through safeguarding, disciplinary or capability procedures, depending on the nature of the concern.

7. Technical Safeguards: Filtering and Monitoring

The school operates a layered technical approach designed to reduce exposure to inappropriate, illegal or harmful material. This includes:

- internet filtering appropriate to age and educational context
- device and network monitoring with proportionate alert systems
- supervision and visibility controls in shared learning spaces.

Filtering and monitoring are reviewed regularly to balance educational access with safeguarding responsibilities. They are used to support pastoral intervention, not to replace supervision or professional oversight.

Where monitoring alerts suggest risk, these are escalated to the DSL for review and, where appropriate, follow-up support.

8. Use of Personal Devices, Mobile Phones and BYOD

Expectations for personal device use are set out in school behavioural procedures and include:

- restrictions in certain areas or times where supervision or safety may be affected
- considerate and respectful use in communal spaces
- restrictions on photographing, recording or sharing images without consent.

Where misuse occurs, responses are guided by proportionality, context and safeguarding risk rather than punishment alone.

9. Remote Learning, Online Platforms and Digital Communication

Staff using digital platforms for learning or communication must:

- apply the same safeguarding standards as in face-to-face settings
- ensure visibility, transparency and appropriate record-keeping
- avoid one-to-one unsupervised digital communication unless authorised and recorded.

Platforms used by the school are assessed for privacy, data protection and safeguarding suitability.

10. Responding to Online Safety Incidents

Concerns may include (but are not limited to):

- cyber-bullying or harassment
- sharing of sexual or indecent images
- grooming or online exploitation concerns
- exposure to extremist or harmful content
- serious wellbeing or mental-health related risk signals.

Staff must report concerns to the DSL without delay. The response may include pastoral support, behaviour processes, safeguarding referral, parental involvement, or external agency engagement.

Where indecent images or illegal activity are suspected, staff must not copy, forward or investigate content themselves; the DSL will follow safeguarding protocols and relevant legal guidance.

11. Training, Awareness and Professional Development

All staff receive regular safeguarding and online safety training appropriate to their role. This includes induction, refresher training and targeted sessions for those with specific responsibilities.

Training emphasises:

- emerging risks and digital trends
- professional conduct and boundary awareness
- recognising vulnerability and harm indicators
- safe reporting and escalation.

Students and parents are included in awareness and information opportunities where appropriate.

12. Data Protection, Privacy and Record-Keeping

Online safety records are stored securely and handled in line with the school's Data Protection and Safeguarding policies. Only authorised staff access case records, and information is shared strictly on a need-to-know basis. Monitoring practices are proportionate, purposeful and respectful of privacy while prioritising student safety.

13.Use of Artificial Intelligence (AI)

Artificial intelligence (AI) is increasingly used in education and everyday life. The school recognises its value for learning and creativity, while also acknowledging potential risks relating to wellbeing, privacy, misinformation and ethical use. AI is therefore approached as both an educational opportunity and a safeguarding responsibility.

Students and staff must use AI in ways that are responsible, respectful and consistent with the school's expectations for academic honesty, professional conduct and data protection. AI may support learning, but it must not replace original thinking or undermine integrity.

Through teaching and pastoral provision, the school supports students to develop informed and balanced attitudes toward AI, including:

- recognising limitations, bias and inaccuracies in AI-generated content
- understanding risks such as misinformation, image manipulation and reputational harm
- protecting privacy and personal data when using AI tools.

Misuse of AI, including plagiarism, harmful content creation or behaviour that leads to safeguarding or wellbeing concerns, will be addressed through appropriate pastoral, behaviour or safeguarding procedures.

The school will review its approach to AI periodically, recognising that technology and associated risks continue to evolve.

14. Audit, Monitoring and Review

The leadership team periodically reviews:

- incident patterns and recurring themes
- effectiveness of filtering and monitoring systems
- training uptake and impact
- student and staff feedback.

Findings inform safeguarding development planning and are reported through appropriate governance channels. The policy is reviewed at least annually, or sooner if technology, guidance or contextual risk changes.

15. Distribution and Access

This policy is available to all staff, students, and parents via the school website and on the school Google drive. Printed copies can be requested from the school reception.