POL/ADMISSION AND WITHDRAWAL:

Policy Title:	Online Safety (E-Safety) Policy
Version:	1.0
Effective Date:	April 2026
Scheduled Review Date:	April 2027
Approved By:	Sydney Atkins Principal

1. Introduction

GEMS Modern Academy is an IB Continuum School with English as the language of instruction. It also offers the CISCE curriculum from Grade 6 to Grade 12. In line with the mission of the school, students are nurtured and encouraged to achieve their ultimate potential, by creating an all-inclusive, student- focused learning environment and providing opportunities for enrichment in the fields of academics, sports and fine arts.

At GEMS Modern Academy - Dubai, we are committed to providing an exceptional educational experience that nurtures academic excellence, character development, and global citizenship. As the only Outstanding-rated Indian/IB curriculum school in Dubai, we recognize that technology plays an integral role in modern education and our students' lives.

2. Purpose

The purpose of this policy is to:

2.1. Safeguard Students: Protect students from harmful or inappropriate online content, contact, conduct, and commerce (the 4Cs of online safety).
2.2. Promote Digital Citizenship: Cultivate responsible, ethical, and respectful digital citizens within our school community.
2.3. Support Families: Partner with parents in digital parenting through open communication, education, and guidance.
2.4. Provide Clear Guidelines: Establish unambiguous expectations for the safe use of technology for students, staff, and parents.
2.5. Ensure Robust Systems: Implement and maintain effective filtering, monitoring, and reporting systems, supported by professional human oversight.

2.6. Address Emerging Risks: Proactively manage risks associated with artificial intelligence, social media, and mobile technology.
2.7. Uphold the GMA Ethos: Ensure our digital environment reflects our core values of academic excellence, integrity, and respect.

Through this policy, we aim to enable our students to grow in confidence, flourish in a connected world, and remain mindful of the choices they make online.

3. Scope

The rationale for this Online E-Safety Policy is to establish a clear framework that protects students from online harm, ensures responsible use of technology, and supports our wider safeguarding responsibilities. By embedding safe and mindful digital practices, we prepare our students not only to succeed academically but also to make positive, responsible contributions to their communities.

Our philosophy extends to digital citizenship, empowering our students with the knowledge and critical thinking skills to navigate the online world safely, responsibly, and ethically. This policy establishes a clear framework to protect our students from online harm, ensures the responsible use of technology, and supports our wider safeguarding responsibilities, in full alignment with UAE regulations and KHDA standards.

We recognize that digital parenting is a shared responsibility between the school and families. Together, we strive to strike the right balance between enabling children to access educational and enriching opportunities whilst safeguarding them from risks of harm.

4. Policy Statements

4.1. **The 4 C's of Online Safety -** We educate our community to recognise and respond to the four categories of online risk (the 4Cs):

Area	Risk	Examples	What it Means
Content	*Child as Recipient*	Illegal, inappropriate or harmful content including: • Explicit adult content, fake news • Racism, misogyny, radicalisation • Self-harm, suicide, extremism	Children may see harmful or age-inappropriate online material.

Contact	*Child as Participant*	Harmful online interaction with others: • Peer pressure, cyberbullying • Adults posing as children • Grooming and exploitation	Children may be approached by strangers or manipulated into sharing personal information online.
Conduct	*Child as Actor*	Personal behaviour that causes harm: • Making, sending explicit images • Online bullying • Online challenges	How children behave online - cyberbullying, sharing images, oversharing, participating in risky challenges.
Commerce	*Child as Consumer*	Risks linked to: • Online gambling • Inappropriate advertising • Phishing and financial scams	Risks from online shopping, scams, in-game purchases or data misuse.

4.1.1. Family Conversation Starters:

a. Content: 'What kind of things do you come across online that make you curious or uncomfortable?'
b. Contact: 'Do you know what to do if someone you don't know messages you?'
c. Conduct: 'How can we show kindness and respect online, even when we disagree?'
d. Commerce: 'Have you ever been asked to buy something or share personal details online?'
e.

4.2. Digital Parenting Partnership: the 5 Steps

GEMS Modern Academy recognizes that today's parental responsibilities include managing children's digital access and online behaviour. We support parents through our Digital Parenting in 5 Steps framework:

Step 1: Open Communication

Be open with your child about the digital world. Discuss possible risks, agree on boundaries, dos and don'ts, and how to ask for help when needed. Children are more likely to seek help if the rule is 'help first, consequences later.'

Step 2: Understanding the Risks

Keep up to date with online risks through reading specialized publications, following subject experts, attending school workshops and speaking to your child. Use the 4Cs framework to recognise and manage risks.

Step 3: Modelling Digital Behaviour

Demonstrate good digital choices through your own relationship with technology. Show balanced use, prioritise real-life interactions, and practice digital citizenship (kindness, responsibility, and commitment to online safety).

Step 4: Parental Control

Filter content and limit access for children by setting permissions and customizing app privacy preferences. Use parental control tools to manage online activity, limit exposure to potential risks, and create a safer digital environment.

Step 5: Monitoring Digital Interactions

Age-appropriate monitoring to ensure children are safe online. Discuss arrangements with your child beforehand - monitoring should be transparent and agreed upon, balancing safety with privacy.

4.3. Online Challenges

Online challenges are activities or dares that children are encouraged to perform, record and share on social media platforms. These can pose serious safeguarding concerns as they:

4.3.1. Normalize and encourage dangerous risk-taking behaviour
4.3.2. May link to cyberbullying through peer pressure
4.3.3. Can be disguised as harmless until someone is hurt
4.3.4. May result in disciplinary consequences or criminal offences
4.3.5. Spread quickly through peer pressure, FOMO, social validation, and viral algorithms

Students and families should be aware of these risks and report any concerning challenges to the school immediately.

4.4. Education and Training

4.4.1. Staff Training: All staff receive e-safety training including understanding of the 4Cs framework and how to support students and families in digital citizenship. Training is part of induction and ongoing professional development.
4.4.2. Parent Education: Parents receive regular guidance on digital parenting through workshops, webinars, and resources aligned with the Digital Parenting in 5 Steps framework and 4Cs of Online Safety.

4.4.3. Student Education: Students receive age-appropriate education on the 4Cs of online safety throughout the curriculum, empowering them to recognise risks and make safe, responsible digital choices.

4.5. Technical Infrastructure, Equipment, Filtering and Monitoring

The school implements a comprehensive Digital Safeguarding 360° Strategy that includes:

4.5.1. Filtering: Blocking access to harmful sites and content on school networks
4.5.2. Monitoring: Identifying when users access or search for harmful content, with AI monitoring tools and DDSO oversight
4.5.3. Reporting: Recording concerns on Guard and monitoring trends on Power BI
4.5.4. Regular Reviews: Audits of safety and security of school technical systems
4.5.5. Data Protection: Personal data cannot be sent over the internet or taken off site unless safely encrypted

4.6. Artificial Intelligence (AI)

4.6.1. AI tools must be used responsibly and for educational purposes only
4.6.2. Students are taught to critically evaluate AI-generated content for potential biases or inaccuracies
4.6.3. AI must not be used to generate harmful or inappropriate content
4.6.4. Personal or sensitive information must never be shared with AI tools

4.7. Communication, Images, and Social Media

4.7.1. Staff-Student Communication
Must only occur via official school systems (e.g., Microsoft Teams or Seesaw) for educational purposes, be professional, and transparent.

4.7.2. Images & Recording
The use of personal devices to take images is prohibited. Images of students must only be taken on school equipment with permission. Students must not take, share, or publish images of others. Misuse is a serious breach and will be addressed under safeguarding and behaviour policies.

4.7.3. Social Media (Staff)
Staff must maintain professional boundaries. They must not reference students, parents, or school matters on personal social media accounts and must ensure their security settings are robust.

4.8. **Responding to Incidents of Misuse**

All incidents will be recorded, investigated, and acted upon proportionately.

4.8.1. Minor Breaches: Addressed through education, pastoral support, and restorative practices.
4.8.2. Serious Breaches: (e.g., cyberbullying, bypassing filters, online challenges) will result in sanctions per the school's behaviour policy, including temporary removal of network access and mandatory training.
4.8.3. Illegal or Severe Safeguarding Breaches: (e.g., grooming, threats, illegal imagery) will be immediately referred to the Designated Safeguarding Lead

(DSL). The school will follow safeguarding procedures and involve external agencies, including the police, where necessary.

5. Responsibilities

5.1. Local Advisory Board (LAB): The LAB is responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the LAB receiving regular information about e-safety incidents and monitoring reports. A member of the LAB has taken the role of E-Safety Lead. The role of the E-Safety Lead will include:

5.1.1. Regular meetings with the Digital Safety Officer
5.1.2. Regular monitoring of e-safety incident logs
5.1.3. Regular monitoring of filtering / change control logs

5.2. Principal and Senior Leaders

5.2.1. The Principal has a duty of care for ensuring the safety (including e-safety) of members of the school community
5.2.2. The Principal and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff
5.2.3. The Principal and Senior Leaders are responsible for ensuring that the Designated Digital Safeguarding Officer and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant
5.2.4. The Principal will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role

5.3. Designated Digital Safeguarding Officer (DDSO)

5.3.1. Is L3 Safeguard trained
5.3.2. Takes day-to-day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
5.3.3. Provides training and advice for staff
5.3.4. Liaises with DSL (Designated Safeguarding Officer) accordingly
5.3.5. Liaises with school technical staff
5.3.6. Reports regularly to Senior Leadership Team
5.3.7. Ensures education around E-Safety addresses the four categories of online risks (4Cs)

5.4. **ICT Engineer:** The ICT Engineer is responsible for ensuring:

5.4.1. That the school's technical infrastructure is secure and is not open to misuse or malicious attack
5.4.2. That the school meets required e-safety technical requirements and any KHDA / other relevant body E-Safety Policy / Guidance that may apply
5.4.3. That users may only access the networks and devices through a properly enforced password protection policy
5.4.4. The Filtering Policy is applied and updated on a regular basis

5.4.5. That they keep up to date with e-safety technical information to effectively carry out their role
5.4.6. That network and internet use is regularly monitored and any misuse reported appropriately

5.5. **Teaching and Support Staff:** Are responsible for ensuring that:
5.5.1. They have an up-to-date awareness of E-safety matters and of the current school online safety policy and practices
5.5.2. They have read, understood and signed the Acceptable Use Policy
5.5.3. They report any suspected misuse or problem to the Designated Digital Safeguarding Officer
5.5.4. All digital communications with students / parents / carers should be on a professional level and only carried out using official school systems
5.5.5. E-safety issues are embedded in all aspects of the curriculum and other activities
5.5.6. Students understand and follow the E-safety and Acceptable Use policies
5.5.7. They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and implement current policies

5.6. **Students**
5.6.1. Are responsible for using the school digital technology systems in accordance with the Acceptable Use Policy
5.6.2. Need to understand the importance of reporting abuse, misuse or access to inappropriate materials
5.6.3. Will be expected to know and understand policies on the use of mobile devices and digital cameras
5.6.4. Should understand the importance of adopting good e-safety practice when using digital technologies out of school

5.7. **Parents / Caregivers:** Parents and caregivers play a crucial role in digital parenting. While many parents may have only a limited understanding of e-safety risks, they remain essential partners in educating and guiding their children. The school will support parents and caregivers through:
5.7.1. Parent sessions and webinars on digital parenting
5.7.2. High-profile events and campaigns (e.g. Safer Internet Day)
5.7.3. Digital Parenting Guidebook and resources
5.7.4. Letters, newsletters, and the school website
5.7.5. Guidance on the 5 Steps of Digital Parenting and the 4Cs of Online Safety

Parents have a duty to report online safeguarding matters to school and actively support the school in promoting good e-safety practice.

6. Acknowledgement and Agreement

I acknowledge that I have thoroughly read and agree to the GEMS Modern Academy - Dubai E-Safety Policy. I will instruct my son/daughter regarding the importance of following all the guidelines included in the agreement, including the 4Cs of Online Safety and the 5 Steps of Digital Parenting.

Parent/Guardian

Name: _____

Signed: _____

Relationship to child: _____

Date: _____

Student

Name: _____

Signed: _____

Form class: _____

Date: _____

7. Monitoring and Review

Signed: _____ Date: _____

Head of Primary

Signed: _____ Date: _____

Deputy Head of Primary

Signed: _____ Date: _____

Head of Secondary

Signed: _____ Date: _____

Principal

Next policy review date: September 2026

8. Associated Policies

This policy works in conjunction with the:

- GEMS Safeguarding Policy
- GEMS Safer Working Practice Guidance
- Behaviour & Anti-Bullying Policies
- Staff Code of Conduct
- Digital Device Responsible Use Agreement (DDRUA) for Students & Parents
- GEMS Digital Parenting Guidebook