

GEMS LEGACY SCHOOL – DUBAI

A Legacy of Empathy, Resilience, Leadership and Sustainable Living

DIGITAL SAFEGUARDING POLICY

Applies To	All Students – KG1 to Grade 11
Curriculum	CBSE, Dubai, U.A.E
Policy Owner	GEMS Legacy School
Effective	Academic Year 2026–2027 Reviewed Annually

1. PURPOSE

GEMS Legacy School (GLS) is committed to safeguarding and promoting the welfare of every student, including within digital environments. This policy ensures the safe, responsible, and ethical use of digital technologies by all members of the school community.

The policy outlines how GLS **prevents, identifies, and responds to digital safeguarding risks**, in alignment with:

GEMS Safeguarding Policy

UAE Federal Laws (including Child Rights Law)

KHDA safeguarding requirements

The welfare and protection of every child remain the highest priority.

2. AIMS

This policy aims to:

Protect students from digital harm, including cyberbullying, online grooming, harmful content, and misuse of technology

Promote a culture of **safe, responsible, and ethical digital behavior**

Ensure digital safeguarding is embedded across:

Curriculum

Pastoral Care

School Culture

Empower students to **recognize risks and report concerns confidently**

3. ROLES AND RESPONSIBILITIES

Designated Safeguarding Lead (DSL)

Overall responsibility for digital safeguarding

Manages all safeguarding concerns and incidents

Liaises with external agencies where required

Digital Safeguarding Policy

Deputy DSL

Supports DSL and ensures continuity of safeguarding processes

Principal / Senior Leadership Team

Ensure implementation and compliance with safeguarding policies

Promote a strong safeguarding culture across the school

IT Department

Maintain filtering, monitoring, and cybersecurity systems

Ensure safe use of digital platforms and infrastructure

All Staff

Must report safeguarding concerns immediately

Always follow GEMS safeguarding procedures

Maintain safe professional digital conduct

Students

Use technology safely and responsibly

Report any concerns immediately

Parents / Guardians

Support safe use of technology at home

Work in partnership with the school to address concerns

4. OBJECTIVES

GLS will:

- Maintain **robust filtering and monitoring systems**
- Deliver **age-appropriate digital safety education**
- Ensure **annual staff safeguarding training**
- Provide clear safeguarding **reporting and response processes**
- Engage parents as partners in digital safety

5. KEY DIGITAL RISKS

GLS identifies five categories of digital risk applicable across all grade levels:

Category	Examples of Risk
Content	Exposure to harmful, inappropriate, extremist, or misleading material
Contact	Online grooming, strangers, unsafe communication
Conduct	Cyberbullying, harassment, sharing harmful content
Privacy	Sharing personal data · Weak passwords · Misuse of AI tools (deepfakes, generative AI)
Commerce	Scams, Phishing, Online Fraud, In-App Purchase



6. STUDENT RESPONSIBILITIES

Students are expected to:

- Use digital technologies safely and responsibly
- Treat others with dignity and respect online
- Not share personal information or credentials
- Not create or share harmful or inappropriate content
- Not record others without consent
- Report concerns immediately to a trusted adult

7. STAFF AND PARENT RESPONSIBILITIES

Staff

All staff will:

- Complete mandatory GEMS safeguarding training annually
- Receive specific training on digital risks, cyberbullying, and online safety
- Be updated regularly on emerging risks including AI technologies
- Report any digital safeguarding concern, regardless of severity, immediately to the Designated Safeguarding Lead (DSL).
- Use only school-approved platforms; submit new platform requests to the Digital Learning Coach one week before intended use.

Parents / Guardians

- Supervise children's technology use at home
- Reinforce safe online behaviour
- Report concerns to the school promptly
- Ensure personal devices used in school are appropriate

8. TECHNICAL SAFEGUARDS

GLS implements:

- Content Filtering
- Blocks access to harmful or inappropriate content
- Regularly reviewed and updated
- Monitoring
- Network activity may be monitored by authorised staff
- Students should not expect privacy on school systems
- Approved Systems
- Only school-approved platforms may be used
- BYOD Controls
- Devices must connect to the filtered school network
- VPN & Circumvention
- Use of VPNs or bypass tools is strictly prohibited

9. DATA PROTECTION AND DIGITAL RESPONSIBILITY

GLS ensures that:

- Student data is handled in accordance with UAE data protection laws
- Personal information is protected from unauthorised access
- Third-party platforms are only used following approval and safeguards



10. ARTIFICIAL INTELLIGENCE AND EMERGING TECHNOLOGIES

- Students will be educated on **ethical and safe use of AI tools**
- Use of AI will be monitored to prevent misuse
- Risks such as misinformation, deepfakes, and plagiarism will be addressed

11. REPORTING AND RESPONDING TO CONCERN

Students can report concerns through:

- Teachers
- School counsellor
- Designated Safeguarding Lead
- Digital reporting channels (where available)

All concerns will:

- Be recorded and reviewed by the DSL
- Follow **GEMS Child Protection Procedures**
- Be escalated where required
- Be handled confidentially and sensitively

Where necessary:

- Parents will be informed
- External agencies may be involved in line with UAE law

12. CYBERBULLYING AND BEHAVIOR

Incidents of cyberbullying will be addressed in line with:

- Safeguarding procedures
- Behaviour Policy
- Anti-Bullying Policy

13. EDUCATION AND STUDENT EMPOWERMENT

GLS will:

- Deliver digital citizenship education through the curriculum
- Conduct assemblies and awareness sessions
- Promote responsible digital behaviour
- Ensure students know:
 - how to stay safe
 - how to report concerns
 - who to approach for help

14. POLICY LINKAGES

This policy should be read alongside:

- GEMS Safeguarding Policy
- Behavior Policy
- Anti-Bullying Policy
- Acceptable Use Policy (AUP)