مدرسة جيمس متروبول
GEMS Metropole School
MOTOR CITY

E-Safety Policy

Reviewed by: Mr. Naveed Iqbal Reviewed Date: April 2026

Next Review: October 2026

Contents

1. Purpose
2. Rationale
3. Scope
4. Definitions
5. School Commitment
6. Leadership and Responsibilities
7. Filtering, Monitoring and Device Management
8. Approved Accounts and Digital Platforms
9. Device Expectations
10. Photography, Video and Student Images
11. The Four Categories of Online Risk
12. Artificial Intelligence and Emerging Technology
13. Social Media and UAE Legislation
14. Curriculum and Student Education
15. Student Leadership
16. Parent Partnership
17. Reporting Concerns
18. Behaviour, Consequences and Support
19. Out-of-School Online Behaviour
20. Staff Training
21. Related Policies
22. Monitoring and Review

1. Purpose

GEMS Metropole School Motor City is committed to providing a safe, secure and positive learning environment in which technology enhances teaching, learning, communication, creativity and innovation.

This policy sets out the school's approach to online safety and digital safeguarding, ensuring that students, staff and families are protected from risks associated with internet use, connected devices, digital communication platforms and emerging technologies.

The school recognises that online safety is a core safeguarding priority.

2. Rationale

Digital technologies create significant opportunities for learning, collaboration and future readiness. However, they may also present risks including harmful content, cyberbullying, scams, grooming, misuse of images, misinformation and inappropriate use of artificial intelligence.

The school therefore adopts a proactive approach built around:

- education
- supervision
- secure systems
- responsible behaviour
- strong safeguarding procedures
- partnership with families

Internet access within school is considered a privilege linked to safe, responsible and respectful use.

3. Scope

This policy applies to:

- all students
- all staff
- contractors, visitors and volunteers where relevant
- parents and caregivers
- school devices, systems and networks
- personal devices brought onto site where permitted
- digital behaviour that affects student welfare, safety, learning or the wider school community

4. Definitions

Online Safety

The safe, responsible and respectful use of technology, devices, platforms and digital communication.

Digital Safeguarding

Protecting children and young people from harm linked to technology or online activity.

Cyberbullying

Repeated harmful behaviour through digital means, including messaging, social media, group chats or image misuse.

Artificial Intelligence (AI)

Technology capable of generating responses, images, text, recommendations or decisions.

Filtering

Systems used to reduce access to harmful, illegal or inappropriate content.

Monitoring

Systems used to identify possible misuse, safeguarding concerns or inappropriate digital behaviour.

5. School Commitment

The school is committed to:

- protecting students from online harm
- promoting respectful digital conduct
- teaching students to become safe digital citizens
- maintaining secure systems
- responding swiftly to concerns
- reviewing emerging risks
- working in partnership with families
- ensuring staff remain up to date

4. Leadership and Responsibilities

Principal and Senior Leadership Team

Will:

- provide strategic oversight
- ensure appropriate resources and systems are in place
- maintain a strong safeguarding culture
- review policy effectiveness annually
- support staff accountability and compliance

Designated Safeguarding Lead (DSL)

Will:

- lead responses to online safety concerns
- ensure incidents are recorded and followed up
- liaise with parents and agencies where required
- monitor patterns and recurring risks
- coordinate support plans

Digital Lead

Will:

- support safe use of educational technology
- review digital trends and risks
- help develop good practice across the school
- work alongside safeguarding and IT teams

IT / Technical Staff

Will:

- maintain secure infrastructure
- operate filtering and monitoring systems
- manage access permissions
- support Jamf and device management systems
- respond quickly to urgent website blocking requests

Staff

Will:

- model professional technology use
- supervise students appropriately
- use approved platforms only
- read and follow acceptable use expectations
- report concerns immediately
- maintain awareness of emerging risks

Students

Will:

- use systems responsibly
- respect others online
- protect passwords and personal information
- report concerns
- follow all device rules

Parents / Caregivers

Are encouraged to:

- support safe use at home
- reinforce respectful behaviour
- monitor age-appropriate access
- work positively with the school

7. Filtering, Monitoring and Device Management

The school uses a range of systems to support safe technology use.

These may include:

- filtered internet access
- monitoring systems
- managed accounts
- mobile device management through Jamf
- app controls
- classroom management tools such as Apple Classroom where appropriate

Students in Years 3-11 must have devices enrolled onto the school management system in order to access internet services in school.

The school maintains a substantial restricted website list, including harmful, inappropriate and unauthorised AI-related websites. Staff may submit requests for websites to be reviewed and blocked rapidly where required.

Filtering and monitoring support safeguarding but do not replace active supervision, staff vigilance or student education.

Passwords must remain secure and users must not share login credentials.

8. Approved Accounts and Digital Platforms

Students must use official school-managed accounts to access school resources, including Microsoft Teams and other approved systems.

Use of personal accounts for school learning is not permitted unless specifically authorised.

Approved platforms may also be used to direct students to safe websites, curated research materials and teacher-approved tasks.

9. Device Expectations

During the school day:

- personal mobile phones are not permitted for use unless specifically authorised
- smart watches are not permitted
- smart glasses are not permitted
- students must follow staff instructions regarding devices
- devices must be used for learning purposes only

Students must not attempt to bypass safeguards through:

- VPNs
- personal hotspots
- tethering
- alternative network routes
- unapproved accounts

Breaches will be managed in line with the Behaviour Policy and may trigger safeguarding review.

10. Photography, Video and Student Images

Photography or video involving students should only take place on authorised school devices such as school-managed iPads.

Personal devices must not be used by staff to capture images or recordings of students.

The school operates image permission systems. A restricted-photo list is maintained to ensure that students whose families have opted out are not included in promotional or social media content.

Unauthorised recording, image misuse or harmful sharing of content will be treated seriously.

11. The Four Categories of Online Risk

Content

Students may encounter:

- pornography
- violent content
- extremist material
- hate content
- misinformation
- self-harm material

Contact

Risks include:

- grooming
- coercion
- unsafe messaging requests
- adults posing as children
- pressure to share personal details

Conduct

Risks include:

- cyberbullying
- harassment
- peer conflict in chats
- image misuse

- Impersonation
- threatening messages

Commerce

Risks include:

- phishing
- scams
- fraud
- gambling
- identity theft
- in-app purchase pressure

12. Artificial Intelligence and Emerging Technology

The school recognises both the opportunities and risks associated with AI.

Students may not access generative artificial intelligence tools until **Year 9 (age 13+)**, unless specifically authorised by the school for educational purposes under staff supervision.

Risks may include:

- inaccurate information
- unsafe advice
- plagiarism or academic dishonesty
- sharing personal data
- deepfake content
- biased or inappropriate outputs

Staff remain professionally responsible for any AI-assisted outputs used in school.

13. Social Media and UAE Legislation

The school supports the UAE's national approach to protecting children online and expects students and families to comply with applicable legislation regarding social media use.

Commented [BRT] [Johnson Hampton] FYI

Commented [SHORT] [pmet, Sheik Jon Brandon]

In line with UAE law:

- Children under the age of 15 must not hold or create personal social media accounts.
- Young people aged 15-16 may only access social media platforms that provide enhanced child protection measures in accordance with UAE regulations.
- Parents and caregivers remain responsible for supervising their child's use of technology outside school and are encouraged to follow national age guidance.

- The school will continue to educate students about responsible digital citizenship and safe online behaviour.

The school's expectations regarding the use of generative artificial intelligence are separate from UAE social media legislation and are outlined in Section 12.

14. Curriculum and Student Education

Online safety is taught through age-appropriate curriculum and pastoral opportunities.

Primary

Online safety is taught as the first computing topic each academic year through Kapow Computing, providing an annual refresher based on changing technologies and emerging risks.

Secondary

Online safety is reinforced through curriculum lessons, assemblies and pastoral messaging.

15. Student Leadership

The school develops Digital Leaders in both Primary and Secondary.

Digital Leaders help model responsible technology use, support peers where appropriate, and contribute student voice on digital matters.

16. Parent Partnership

The school values partnership with families and may provide workshops, guidance or awareness sessions throughout the year.

This has included sessions on:

- keeping children safe online
- risks linked to artificial intelligence

While home device use remains a parental responsibility, the school encourages families to consider age guidance carefully before allowing access to platforms.

17. Reporting Concerns

Any online safety concern should be reported immediately.

Examples include:

- cyberbullying
- threatening messages
- scams
- harmful content
- image misuse
- suspected grooming
- device misuse
- AI misuse causing harm

Concerns are recorded through the school safeguarding platform and escalated appropriately. Parents may be contacted as part of investigation or support processes.

Where concerns relate to staff conduct or malpractice, additional reporting routes including the GEMS Whistleblowing Policy may apply.

18. Behaviour, Consequences and Support

Responses may include:

- education and restorative conversations
- behaviour sanctions
- device restrictions
- confiscation where appropriate
- parent meetings
- safeguarding support
- counselling or pastoral intervention

Responses will be proportionate to age, intent, severity and risk.

19. Out-of-School Online Behaviour

Where behaviour outside school affects student welfare, relationships, learning or safety within school, the school may investigate and provide support.

The school may work with families to restore a safe learning environment.

Families may also be reminded that some online behaviours may breach applicable UAE laws.

20. Staff Training

All staff complete safeguarding training, including induction or Level 1 safeguarding expectations.

Annual corporate training is also completed.

Updates regarding AI, emerging risks and online safety may be shared through staff briefings.

Safeguarding team members complete refresher training to remain current with evolving threats and practice.

21. Related Policies

This policy should be read alongside:

- Safeguarding Policy
- Behaviour Policy
- Anti-Bullying Policy
- Acceptable Use Policies
- Data Protection / Privacy guidance
- Staff Code of Conduct

22. Monitoring and Review

This policy will be reviewed annually, or sooner where technology, safeguarding risks or organisational expectations change.

Strategic oversight remains with the Principal and Senior Leadership Team.

Operational implementation is led by the DSL and Digital Lead.