



مدرسة جيمس متروبول
GEMS Metropole School
MOTOR CITY

B.Y.O.D



Reviewed by	Mr. Naveed Iqbal	Reviewed Date	October 2025
Next Review	October 2026		

Table of Contents	
Purpose.....	2
Rationale.....	2
Scope	2
Device Setup, E-Safety and Costs	2
Artificial Intelligence.....	3
Monitoring and Filtering.....	4
Parent Responsibilities	4
Loss, Damage and Liability.....	4
Breaches and Consequences	4
Related Policies	4
Review	4
Required Devices by Year Group.....	4
Minimum Specifications	4
Acceptable Use of Devices.....	5

Purpose

GEMS Metropole School Dubai recognises that personal technology can significantly enhance learning, organisation, collaboration, creativity and communication when used responsibly. This policy sets out the expectations for students who bring personal devices to school and access school systems.

Rationale

The school is committed to future-ready learning environments supported by high-quality technology. Clear expectations are required to ensure devices are used safely, respectfully and for educational purposes.

Scope

This policy applies to all students bringing devices onto campus, connecting to school Wi-Fi, accessing school platforms or using devices in a way that affects school life.

Device Setup, E-Safety and Costs

Students in Years 3-11 must have eligible devices enrolled onto the school device management/e-safety platform before accessing school internet services.

E-safety installation cost: 240AED.

Transfer to a replacement device: 120AED.

- **New** devices may be purchased directly from our [MTS E-Store](#) with e-safety pre-installed.
- **Existing** compatible devices can have e-safety installed onto them. To purchase e-safety for an existing device, [please click here](#)
- Where a student changes device, settings must be **transferred** to the new device. To purchase the transfer of e-safety, [please click here](#)

For support, families should contact JTRS on 04 338 0990 or info@jtrs.ae.

Alternatively, please visit the IT department with proof of payment for support.

E-Safety Restrictions for Students Working From Home

E-safety is controlled through time-based restrictions and remains active during school hours. If a child is absent from school, requests to remove e-safety restrictions will generally not be approved due to the significant workload involved in managing individual devices across the MDM.

During school hours, the iPad functionality provided to students at home remains appropriate for educational use and helps to mitigate safeguarding risks. As students are still engaged in online learning, additional apps or unrestricted access should not be required during this time.

Exceptions will only be considered in circumstances where a student is absent for a sustained period of time (in excess of two weeks). In these cases, a formal request outlining the start and end dates must be submitted to the IT team.

Restrictions

During school hours, the following restrictions are currently applied:

- Only approved school apps are visible
- iMessage and FaceTime are disabled
- New App Store purchases are restricted
- VPN creation is blocked
- “Erase All Content and Settings” is disabled

The MDM profile operates under Apple’s strict privacy framework. The school cannot access personal data, messages, photos, accounts or browsing content on the device. You can also review the active profile configuration at any time by navigating to:
Settings > General > Device Management

Daily Expectations

Students must bring devices fully charged, use them for learning purposes, follow staff instructions, join Apple Classroom when requested, keep passwords private and store devices safely.

Artificial Intelligence

AI tools may only be used when age-appropriate (13+), approved by the school and directed by staff. Misuse includes plagiarism, unsafe prompts, sharing personal data or generating harmful content.

Monitoring and Filtering

The school uses recognised safeguarding, filtering and monitoring systems including device management tools. Use of school systems may be monitored where appropriate in line with safeguarding and legal responsibilities.

Parent Responsibilities

Parents are expected to provide a suitable device, ensure it is charged and protected, support respectful behaviour online, monitor appropriate home use and work positively with the school where concerns arise.

Loss, Damage and Liability

Students remain responsible for the care and security of personal devices. The school accepts no liability for loss, theft or accidental damage unless required by law.

Breaches and Consequences

Breaches may result in warning, confiscation, restricted access, parent meetings, behaviour sanctions, safeguarding review or further disciplinary action.

Related Policies

This policy should be read alongside the E-Safety Policy, Behaviour Policy and Safeguarding Policy.

Review

This policy will be reviewed annually or sooner where operational or safeguarding needs require.

Required Devices by Year Group

Year Group	Device required
Years 3-6	Apple iPad
Years 7-9	Apple iPad
Years 10-11	Apple MacBook
Years 12-13	Flexible device choice

Minimum Specifications

The following devices are compatible with iPadOS 26, macOS, and future operating system upgrades:

- iPad (8th Generation and later)
- iPad Air (3rd Generation and later)
- iPad mini (5th Generation and later)
- iPad Pro 11-inch (1st Generation and later)
- iPad Pro 12.9-inch (3rd Generation and later)
- iPad Air M2/M3/M4 models
- iPad Pro M4/M5 models
- iPad (A16)
- iPad mini (A17 Pro)
- MacBook Pro and MacBook Air (released in 2020 and later)

Devices below these specifications will experience reduced performance, limited application compatibility, and increasing security and support risks over time.

Acceptable Use of Devices

Students may use personal devices in school to support learning, organisation and communication where authorised by staff.

Permitted uses include:

- Accessing teacher-directed learning resources
- Completing assignments and classwork
- Research using approved and appropriate sources
- Collaborating through approved school platforms
- Creating presentations, documents or academic work
- Using approved educational applications

Students must:

- Follow staff instructions immediately
- Use respectful language and conduct online
- Keep passwords and login details private
- Protect personal information and the privacy of others
- Use devices only when permission has been given

- Report concerns, misuse or unsafe content promptly

Students may not:

- Play games during learning time unless authorised
- Access social media or personal messaging platforms during the school day
- Photograph, record or share images of others without permission
- Download unauthorised applications or software
- Attempt to bypass filtering, monitoring or security controls
- Use Artificial Intelligence tools inappropriately or dishonestly

Failure to follow these expectations may result in sanctions in line with the Behaviour Policy and BYOD procedures.