مدرسة جيمس كامبردج العالمية أبوظبي
GEMS Cambridge International School
ABU DHABI

# BRING YOUR OWN DEVICE (BYOD) POLICY

## Policy Information

| Item | Detail |
|---|---|
| **Policy Title** | Bring Your Own Device (BYOD) Policy |
| **School** | GEMS Cambridge International School Abu Dhabi |
| **Policy Type** | Student Policy |
| **Approved By** | Principal / CEO |
| **Effective From** | Academic Year 2026-27 |
| **Review Cycle** | Annual review |
| **Formal Review Date** | August 2028 or earlier if required |
| **Policy Owner** | Principal / CEO |

## 1. Purpose

GEMS Cambridge International School Abu Dhabi (CIA) recognises that technology can enhance learning, creativity, communication, accessibility and student engagement when used responsibly and safely.

This policy establishes the expectations, responsibilities and safeguards governing the use of personally owned digital devices by students.

The policy aims to: support teaching and learning, promote safe and responsible digital behaviour, protect students' wellbeing and privacy, safeguard school systems and information, strengthen cybersecurity and data protection, support academic integrity, provide clear procedures for reporting concerns and incidents; and ensure compliance with applicable GEMS, ADEK and UAE requirements. Access to school networks, systems and digital services is a privilege, not an entitlement, and is conditional upon compliance with this policy.

## 2. Scope

This policy applies to all CIA students using personally owned or school-authorised devices: on school premises, during the school day, on school transport where school rules apply, during educational visits, trips, competitions and extracurricular activities, during online or distance learning, when accessing school accounts, platforms or systems; and whenever technology is being used for school-related purposes.

The policy applies to: laptops, tablets, mobile phones, smart watches, SIM-enabled devices, internet-connected devices, peripherals and digital accessories; and future technologies capable of creating, storing, processing, recording or sharing information.

Where school-issued or school-loaned devices are provided to students, the safeguarding, behaviour, acceptable-use and digital-safety requirements contained within this policy apply equally unless a more specific school procedure exists.

Staff and visitor device use is governed through separate GEMS and CIA policies.

## 3. General Principles

Student use of technology must always: support learning, be age appropriate, protect the safety and wellbeing of all users, respect the rights, dignity and privacy of others, comply with school safeguarding requirements, support academic honesty, protect school information and systems, comply with UAE laws and cultural expectations; and follow staff instructions.

A student may be instructed at any time to: stop using a device, close applications, secure a device, switch off a device; or temporarily surrender a device in accordance with school procedures.

## 4. Approved Devices and Technical Requirements

The school will determine which categories of devices may be used in each phase or year group.

CIA may publish separate technical requirements detailing: approved device types, minimum operating systems, browser requirements, security-update requirements, antivirus requirements where applicable, network compatibility requirements, battery expectations, storage requirements, charging expectations; and protective case requirements.

Students and parents are responsible for ensuring that devices: are in good working order, are updated, use a secure password or PIN, have appropriate security protection, arrive sufficiently charged, comply with school requirements; and do not contain software intended to attack, bypass or interfere with systems or networks. Failure to meet technical requirements may result in loss of network access.

## 5. Permitted Use

Students may use an authorised device when directed or approved by a teacher for purposes including: research, classwork, coursework, homework, project work, digital collaboration, approved educational software, digital textbooks, assistive technologies, approved assessments; and approved AI-supported learning.

During lessons, students must: follow teacher instructions, use only approved resources, remain on task, keep devices available for supervision, stop use immediately when instructed; and avoid distracting themselves or others.

## 6. Prohibited Use

Students must not: disrupt teaching and learning, access inappropriate content, engage in cyberbullying, harass, threaten or intimidate others, impersonate another individual, access another person's account, share passwords, attempt unauthorised access to systems or information, install unauthorised software, conduct network scanning or hacking activities, gamble, stream non-educational content, use non-educational social media, spread misinformation, misuse AI, cheat or plagiarise, disclose confidential information, transfer school information to personal services; or use technology in ways that breach school expectations or applicable law.

## 7. VPNs and Security Bypass Tools

Students must use only authorised school networks.

Students must not use: VPNs, proxy services, anonymising services, personal hotspots, tethering, alternative DNS services; or any technology intended to bypass school filtering or monitoring. Use of mobile data to avoid school safeguarding controls is prohibited.

## 8. Mobile Phones, Smart Watches and SIM-Enabled Devices

Personal mobile phones are not authorised for student use during the school day.

Exceptions may be approved: for a specific learning activity, for a documented medical need, for an accessibility need; or for a safeguarding requirement. Where an exception does not exist, devices must remain secured and unused. Smart watches and SIM-enabled devices must have communication functions disabled while on site unless a formal exception applies. Mobile phones and smart watches are not considered standard learning devices within the school's BYOD programme.

## 9. Photography, Audio, Video and Recording

Students must not photograph, film, audio-record, screen-record, livestream or publish content involving: students, staff, visitors, school documents, school systems, confidential information; or school activities without explicit permission.

Students must not create or distribute: harmful recordings, humiliating content, manipulated media, deepfakes, recordings of behavioural incidents, examination materials, safeguarding-related content; or confidential information.

## 10. Social Media

Students may not access social media: during the school day, through school systems, through school networks; or during school-supervised activities unless explicitly authorised for educational purposes.

Students must not: create accounts representing the school, present personal opinions as official school communication, publish confidential information, upload unauthorised images or recordings; or engage in harmful, threatening or discriminatory online behaviour.

## 11. Safeguarding Responsibilities

Students must: use devices safely and responsibly, protect personal information, keep passwords secure, communicate respectfully, use approved platforms, report concerns immediately; and follow staff guidance.

Students must immediately report: harmful content, cyberbullying, suspicious communication, scams, phishing attempts, account compromise, inappropriate requests, safeguarding concerns; or anything online causing concern or distress. Students will not be disadvantaged for making genuine safeguarding reports.

## 12. Artificial Intelligence and Digital Learning Tools

Students may use AI tools only when: authorised by the school, approved under applicable CIA and GEMS processes, approved by the teacher, used for a defined learning purpose, appropriate safeguards are in place; and students comply with teacher instructions. Students may only use AI tools specifically authorised by the school for learning activities. Personal AI subscriptions, independently created AI accounts and publicly available consumer AI tools do not automatically become approved for school use.

Students must not use AI to: cheat, plagiarise, fabricate information, impersonate others, bypass assessment requirements, generate harmful content, create deepfakes, spread misinformation, infringe copyright; or misrepresent authorship. AI must supplement learning rather than replace student thinking, creativity and effort.

## 13. AI Consent and Personal Data

Agreement to this policy does not constitute consent for a specific AI platform to process student data.

Where separate consent is required, the school will obtain parent approval through an approved process.

Students must not upload or enter personal, school or family information into unapproved AI tools or digital services.

## 14. Academic Integrity and Copyright

Students must: produce authentic work, acknowledge sources appropriately, comply with assessment rules, follow teacher instructions, respect copyright, respect intellectual property; and accurately declare use of AI where required. The use of digital tools does not remove student responsibility for the accuracy and authenticity of submitted work.

## 15. Data Protection and Privacy

Students must: protect personal information, protect school information, avoid sharing confidential information, use only approved systems; and report concerns immediately.

Students must immediately report: lost devices, stolen devices, compromised accounts, privacy breaches, accidental disclosure, suspected data leakage, phishing incidents; and unauthorised access. Students must immediately report any lost, stolen or unaccounted-for personal device brought onto the school site, whether or not school information is stored on that device.

## 16. Accessibility and Additional Learning Needs

CIA will provide reasonable adjustments where required.

Assistive technologies and accessibility arrangements may be approved through: documented learning plans, medical plans, safeguarding arrangements; or authorised school processes. No student will be disadvantaged academically because their

family does not own a suitable digital device. Where a personal device is required, the school will consider reasonable alternative arrangements subject to available provision.

## 17. Digital Wellbeing

CIA promotes healthy, balanced and age-appropriate use of technology.

Technology should support: learning, creativity, wellbeing, relationships; and personal development.

The school may provide guidance regarding: healthy screen use, sleep and technology, digital resilience, safe online behaviour, social media use, responsible gaming, digital distraction management; and balanced use of online and offline activities. Where concerns exist regarding excessive or harmful technology use, the school may implement appropriate wellbeing, behaviour, safeguarding or pastoral interventions.

## 18. Monitoring and Privacy

CIA applies filtering, monitoring and access controls to school systems and networks.

The school may monitor activity conducted through: school accounts, school systems, school networks; and authorised learning platforms.

Monitoring may occur for: safeguarding, cybersecurity, compliance, investigation, wellbeing, operational security; and protection of the school community. The school does not routinely monitor personal content unrelated to school activity stored on private devices.

## 19. Digital Incidents

Digital incidents include: cyberbullying, misuse of AI, privacy breaches, inappropriate content, phishing, malware, data loss, compromised accounts, unauthorised access, harmful communications; and attempts to bypass school controls. Incidents must be reported immediately.

The school will: investigate, preserve evidence, support affected students, notify parents where appropriate, follow safeguarding procedures, follow cybersecurity procedures, retain records; and escalate matters to external authorities where required. Each formal digital incident will be recorded and reviewed by the Principal/CEO and retained in accordance with applicable records requirements.

## 20. Consequences for Misuse

Misuse may result in: warnings, restorative action, removal of device privileges, withdrawal of network access, temporary confiscation, parental contact, behavioural interventions, safeguarding interventions, disciplinary action, referrals to GEMS procedures; or referral to relevant authorities where required.

## 21. Parent and Guardian Responsibilities

Parents are expected to: support this policy, discuss expectations with their child, monitor appropriate device use outside school, use parental controls where available, monitor social-media use, ensure devices meet requirements, cooperate with investigations; and report concerns promptly. Parents should ensure appropriate insurance and protection arrangements for student devices.

## 22. Loss, Damage and Liability

Personal devices are brought to school at the owner's risk.

CIA does not provide insurance for personal devices and is not responsible for: maintenance, repair, upgrades, accessories, charging provision; or personal data backups. Families are encouraged to insure devices appropriately.

## 23. Communication, Publication and Age-Appropriate Guidance

This policy will be: published through school channels, made available to parents, referenced in school guidance, supported through digital citizenship education; and reviewed annually.

CIA will provide age-appropriate guidance for: FS1-Year 2, Years 3-7; and Years 8-13. These guidance documents will be reviewed annually to ensure continued alignment with regulatory requirements and student developmental needs. Parents will have access to the full policy.

## 24. Training

Students will receive guidance on: digital safety, cybersecurity, privacy, safeguarding, responsible AI use, academic integrity, cybersecurity threats, online communication; and reporting concerns. Appropriate training will be provided before students use school-approved AI learning tools.

## 25. Governance and Review

The Principal/CEO retains overall responsibility for implementation.

The policy will be monitored through: safeguarding records, behaviour records, incident records, digital wellbeing information, cybersecurity information, audit findings, parent feedback, student feedback; and regulatory updates. The policy will be reviewed annually and formally renewed no later than August 2028.