



Madar International School

Students' BYOD Policy, Device Access, and Acceptable Use Guidelines

2026 – 2027

Policy Title: Students' BYOD Policy, Device Access and Acceptable Use Guidelines					
Policy Ref:	Revision	Review Date	Reviewed by	Signature	Date of Next review
BD101	1.0	13 th August 2026	Ms. Sanaa Tabet		15 th March 2026

Table of Contents

1. Our Vision, Mission, and Core Values	2
Our Vision	3
Our Mission.....	3
Our Core Values	3
2. Introduction and Rationale	4
Introduction	4
Rationale.....	5
3. Scope.....	6
4. Eligibility and Device Requirements.....	8
5. Device Access and Connectivity	12
6. Student Responsibilities	15
7. Parent and Guardian Responsibilities.....	18
8. School Responsibilities	20
9. Acceptable Use Guidelines.....	25
10. Acceptable Use: Digital Wellbeing	31
11. Monitoring, Prohibited Use and Consequences	34
12. Agreement and Acknowledgement	37
Parent/Guardian Acknowledgement and Consent.....	39

1. Our Vision, Mission, and Core Values

Our Vision

Madar International School's vision is to be a leader in inspiring and shaping tomorrow's innovative global leaders by facilitating their holistic development within the emerging global knowledge economy.

Our Mission

Our mission is to inspire students to achieve their highest levels of intellectual and personal development through comprehensive, technology-enabled educational programmes delivered by dedicated teachers.

Definitions of Our Mission

- **Intellectual development:** Developing students' knowledge, curiosity, critical thinking, creativity, problem-solving skills, and capacity to become independent, lifelong learners.
- **Personal development:** Supporting students to develop confidence, character, wellbeing, resilience, responsibility, and the social and emotional skills required to thrive.
- **Comprehensive educational programmes:** Providing a broad, balanced, and inclusive education that supports students' academic, personal, social, physical, and future-readiness needs.
- **Technology-enabled education:** Using digital technologies, data, and artificial intelligence purposefully, safely, and ethically to enhance teaching, learning, communication, collaboration, and access to educational opportunities.
- **Dedicated teachers:** Educators who maintain high expectations, respond to students' individual needs, continually develop their professional practice, and are committed to every student's progress and wellbeing.

Our Core Values

At Madar International School, we are guided by the following core values:

- **Respect:** Treating others with dignity and valuing their feelings, beliefs, and differences.
- **Compassion:** Caring about others and offering support when needed.
- **Mercy:** Demonstrating forgiveness, empathy, and understanding.
- **Belonging:** Ensuring that every member of the school community feels accepted, valued, and included.
- **Tolerance:** Accepting and appreciating people with different views, backgrounds, cultures, and traditions.
- **Kindness:** Acting with care, generosity, and consideration towards others.

- **Collaboration:** Working effectively with others to achieve shared goals.
- **Leadership:** Guiding and inspiring others through positive actions and personal examples.
- **Global Understanding:** Developing awareness of and respect for diverse cultures, perspectives, and global issues.

2. Introduction and Rationale

Introduction

Madar International School is committed to creating a connected, innovative and future-focused learning environment in which technology enhances teaching and learning and supports every student's intellectual and personal development.

The Bring Your Own Device (BYOD) programme enables students to use an approved personal learning device to access our learning environment, other school-approved digital platforms, learning resources, and applications. Through purposeful use of technology, students will be able to participate in interactive learning experiences, communicate, and collaborate with others, create and submit work, receive feedback, and continue their learning both inside and outside the classroom.

The programme also supports the development of important future-ready skills, including creativity, critical thinking, problem-solving, communication, collaboration, digital literacy, and the safe, ethical, and responsible use of artificial intelligence.

This policy establishes the expectations and conditions governing the use of personal devices at Madar International School. It:

- defines the responsibilities of students, parents and guardians, staff, and the school;
- establishes standards for the safe, secure, responsible, and educational use of devices;
- sets out the requirements for accessing the school network, learning environment and other approved digital services; and
- supports the school's safeguarding, cybersecurity, data protection, and acceptable use responsibilities.

The policy applies to all students in Grades 1–12 and covers the use of personal learning devices on school premises; through the school's network, systems, or digital platforms; during school-related activities, trips and events; school resources, or services from outside the school.

Compliance with this policy, the school's minimum device specifications and all related safeguarding and acceptable-use requirements is a condition of connecting a personal device to the Madar International School network or using it for school-related learning.

Rationale

At Madar International School, technology-enabled education means using digital technologies, data, and artificial intelligence purposefully, safely, and ethically to improve teaching, learning, communication, collaboration, and access to educational opportunities.

The BYOD programme forms part of the school's wider digital transformation and supports the establishment of a consistent, secure, and inclusive digital learning environment across Grades 1–12. It is founded on the following principles:

- **Alignment with Madar's Vision, Mission, and Core Values**
The programme supports Madar's mission to provide comprehensive, technology-enabled educational programmes and to prepare students to become innovative global leaders. Students are expected to demonstrate the school's values of respect, compassion, mercy, belonging, tolerance, kindness, collaboration, leadership, and global understanding in all digital interactions.
- **Purposeful Teaching and Learning**
Personal devices provide students with timely access to digital learning resources, creative and collaborative tools, assessment activities, and teacher feedback. Technology will be selected and used where it adds educational value and supports clearly defined learning outcomes.
Devices will complement, rather than replace, effective teaching, discussion, handwriting, practical learning, physical activity, and face-to-face interaction.
- **Consistency Between School and Home Learning**
Using the same device at school and at home gives students consistent access to their learning environment, school resources, and their own work. Familiarity with the device and its learning tools can reduce disruption, support continuity and help students become increasingly organized, responsible and independent learners.
- **AI Literacy and Future-Ready Skills**
Following the introduction of ADEK's AI Literacy Framework, Abu Dhabi private schools are expected to begin implementation from 31 August 2026. Madar's BYOD programme will provide students with appropriate access to the digital tools needed to develop AI literacy and to use artificial intelligence safely, ethically, critically and responsibly. This direction also supports the ambitions of the We the UAE 2031 vision by preparing young people to contribute to an innovative, digitally enabled and knowledge-based society.
- **Digital Citizenship, Safety and Safeguarding**

Regular, supervised use of technology allows responsible digital citizenship to be taught and reinforced through everyday learning. Students will learn to protect their privacy and personal information, evaluate digital content critically, communicate respectfully, respect intellectual property and report unsafe or inappropriate online behavior. All device use must comply with school policies, safeguarding requirements and applicable UAE laws.

- **Age-Appropriate and Balanced Use**

The frequency, duration and purpose of device use will be appropriate to students' ages, developmental needs and learning objectives. Teachers will determine when devices should and should not be used during lessons.

- **Consistency, Security and Effective Support**

Clear minimum device specifications, approved applications and connectivity requirements help provide a consistent learning experience and enable the school to manage its network and technical support effectively.

Only devices that meet the school's published requirements may connect to the school network. The school may restrict or remove access where a device presents a security risk, disrupts learning or is used in breach of this policy.

- **Inclusion and Equitable Access**

Madar International School is committed to ensuring that students can participate meaningfully in digital learning. The school will work with families where access to a suitable device presents a genuine difficulty and will determine appropriate support arrangements according to individual circumstances and available school resources. Reasonable adjustments will also be considered for students with additional learning needs, in consultation with the school's inclusion team and parents or guardians.

3. Scope

This policy applies to all students in Grades 1–12 participating in the Madar International School BYOD programme. It governs the use of approved personal learning devices for school-related purposes, whether the device is used on or off the school premises.

Devices Covered

This policy applies to laptops, MacBooks, iPads, and any other personal computing devices approved by the school and included in the relevant Madar BYOD Minimum Device Specifications.

Mobile phones, smartwatches, gaming devices, and other personal electronic devices are not approved BYOD learning devices unless their use has been expressly authorized by the school for a specific educational or accessibility purpose.

Permitted Use

Personal devices may be used to:

- access Toddle and other school-approved platforms, systems, applications and digital resources;
- create, complete, store and submit learning activities and assessments;
- communicate and collaborate for educational purposes;
- receive feedback and monitor learning progress; and
- develop digital literacy, AI literacy, and other future-ready skills.
- Devices must only be used under the direction of a member of staff and for authorized educational purposes during lessons and school activities.

Locations and Activities

This policy applies when personal devices are used:

- in classrooms and other areas of the school;
- during co-curricular and extracurricular activities;
- on school transport, where applicable and permitted;
- during school trips, excursions, competitions and off-site events;
- while connected to the school's Wi-Fi network or accessing its digital systems;
- when accessing school-provided accounts, platforms or resources from home or another location; and
- during any activity undertaken in connection with Madar International School.

People Covered

This policy establishes responsibilities for:

- students, as the users of approved personal learning devices;
- parents and guardians, as the owners or custodians of devices and partners in supporting safe and responsible use;
- teachers and other staff, who direct, supervise and monitor the educational use of devices; and
- School leaders and IT staff, who manage access, security, technical requirements, monitoring and compliance.

Period of Application

The policy applies whenever a personal device:

- is brought onto school premises;
- is connected or attempts to connect to the school network;
- accesses a school account, platform, system or digital resource; or
- is used as part of a school-related learning activity, event or communication, whether during or outside normal school hours.

Relationship with Other School Policies

This policy must be read and applied in conjunction with the following Madar International School policies:

- *Behavior Management Policy*, which governs student conduct and the consequences of inappropriate device or technology use;
- *Academic Integrity Policy*, which governs authentic authorship, acknowledgement of sources, collaboration, assessment conduct, plagiarism, and the responsible use of artificial intelligence;
- *Child Protection and Safeguarding Policy*, which governs the protection of students from harm, including online abuse, exploitation, inappropriate content, cyberbullying and unsafe digital communication; and
- *Teaching and Learning Policy*, which governs the purposeful, age-appropriate and balanced use of technology to support curriculum delivery and student learning.

The policy will also be implemented in accordance with applicable UAE legislation, ADEK requirements, and school procedures relating to cybersecurity, data protection, online safety, and digital safeguarding.

Compliance

Compliance with this policy and the school's minimum device specifications is a condition of connecting a personal device to the Madar International School network and participating in the BYOD programme. Where a device creates a security risk, disrupts teaching and learning or is used in breach of this policy, the school may:

- direct the student to stop using the device;
- temporarily restrict or remove access to the school network, accounts or digital services;
- require the device to be removed from the school premises; and/or
- apply appropriate support, intervention or consequences in accordance with the Behavior Management Policy and other relevant school policies.

Any response will take account of the student's age, the nature and seriousness of the incident, previous incidents, safeguarding considerations and the need to maintain access to learning.

4. Eligibility and Device Requirements

Participation in the Madar International School BYOD programme applies to all students in Grades 1–12. To participate, students must bring an approved personal learning device that:

- is appropriate for their grade level;
- meets the current Madar BYOD Minimum Device Specifications;
- can connect securely to the school's wireless network;
- supports Toddl and other school-approved applications and platforms;

- is maintained in safe and functional condition; and
- is used in accordance with this policy and all related school policies.

Meeting the minimum device requirements makes a device eligible for use but does not automatically grant access to the school network. Network and system access remain subject to the school's security, safeguarding and technical requirements.

Grades 1 to 4 Device Specification

Students in Grades 1 to 4 must bring an iPad that meets the school's published minimum specifications.

Component	Minimum requirement	Recommended for a new purchase
Device type	iPad IOS 15.5 minimum / 18+ recommended Android 11 or later	iPad IOS 15.5 minimum / 18+ recommended Android 13 or later
Operating system	iOS 15.5 or later Android 11 or later	6 GB or more iOS 18 Android 13 or later
Memory	4 GB iPad 10th generation or later, running iPadOS 15.5 or later	6 GB or more iPad 10th generation or later, running iPadOS 15.5 or later
Storage	64 GB	128 GB or more
Wi-Fi	Dual-band Wi-Fi 6 (802.11ax)	Wi-Fi 6 or later
Screen	10 inches or larger	10.9–11 inches
Camera and microphone	Built in	Built in
Battery	6 – 8 hours	6 – 8 hours
Protection	Robust protective case	Robust case with screen protection
Keyboard	Optional for Grade 1 and 2 Recommended for Grades 3 to 5	Optional for Grade 1 and 2 Recommended for Grades 3 to 5
Toddle access	Toddle Student app and current supported browser	Toddle Student app and current supported browser
Accessories	Headphones with Mic Protective case and screen protector	Headphones with Mic Protective case and screen protector
Accidental Damage Insurance	Highly recommended	Highly recommended

Grade 5 Transition Phase

Grade 5 is a transitional year and students may bring either:

- an iPad; or

- a Windows laptop or MacBook.

The device must meet the school's published minimum specifications and be capable of accessing all required learning platforms and applications.

From Grade 6 onwards, students will be expected to use a Windows laptop or MacBook in accordance with the school's BYOD device requirements. Families purchasing a new device for a Grade 5 student are advised to purchase a compliant Windows laptop or MacBook because these devices will continue to meet the student's requirements in Grades 6 to 12.

Grades 6–12 Device Specification

Students in Grades 6 to 12 must bring a laptop that meets the school's published minimum specifications.

Component	Minimum requirement	Recommended for a new purchase
Device	Windows laptop or MacBook	Windows laptop or MacBook
Processor	Intel Core i5 generation 8+ OR AMD Ryzen 3 OR Apple M1 or equivalent	Intel Core i5 generation 8+ OR AMD Ryzen 5 OR Apple M-series or better
Memory	8 GB RAM	16 GB RAM
Storage	256 GB SSD	512 GB SSD
Display	12 inches or larger; minimum 1366 × 768	13–15 inches; Full HD or better
Wi-Fi	Dual-band Wi-Fi 6	Wi-Fi 6E or Wi-Fi 7
Operating system	Supported Windows 11 or macOS (latest version)	Supported Windows 11 or macOS (latest version)
Camera and microphone	Built in	Built in
Battery	At least 8 hours under normal use	10 hours or more
Protection	Protective sleeve or laptop bag	Protective sleeve/bag and accidental-damage cover
Accidental Damage Insurance	Highly recommended	Highly recommended

Device Condition and Daily Readiness

All students must bring their approved device to school each day unless instructed otherwise by the school. The device must be:

- fully charged at the beginning of the school day;
- clearly labelled with the student's name and grade or class;
- protected by an appropriate case, sleeve or bag;
- free from faults that could make it unsafe to use;
- configured with all required school-approved applications and updates; and
- able to connect to the school network and access required learning platforms.

Ownership, Insurance and Maintenance

The device remains the property and responsibility of the student and their parent or guardian.

Families are responsible for:

- purchasing and maintaining the device and required accessories;
- arranging repairs when required;
- backing up personal and school-related work;
- protecting the device against loss, theft and accidental damage; and
- ensuring that warranty or insurance arrangements are appropriate for daily school use.
- Accidental-damage insurance is highly recommended.

Approval and Compatibility

The school reserves the right to inspect a device's technical configuration for compatibility, connectivity, cybersecurity and safeguarding purposes before permitting access to the school network or digital services.

A device may be refused or have its access restricted if it:

- does not meet the published minimum specifications;
- uses an unsupported or insecure operating system;
- cannot run required school applications;
- has been modified in a way that compromises its security;
- presents a risk to the school network, systems or users; or
- is used in breach of this policy.

The school may update its minimum device specifications as curriculum, security and technical requirements evolve. Reasonable notice will be provided where a change could require families to replace or significantly upgrade a device.

Accessibility and Individual Needs

Where a student requires an alternative device, assistive technology or adjusted configuration because of an identified learning, accessibility or medical need, appropriate arrangements will

be agreed with the Inclusion Team, relevant school leaders and the student's parent or guardian.

5. Device Access and Connectivity

To maintain a safe, secure, and reliable digital learning environment, all personal learning devices used at Madar International School must comply with the following access, connectivity, and cybersecurity requirements.

School Network Access

- Students must connect only to the Student BYOD Wi-Fi network when using personal devices on school premises.
- Students must not connect personal devices to staff, administrative, guest or other restricted school networks unless expressly authorized by the IT Department.
- Personal hotspots, mobile data connections and tethering must not be used on school premises unless specifically authorized by a member of staff for an approved educational, accessibility or emergency purpose.
- Internet access provided through the school network will be filtered, logged and monitored in accordance with the school's safeguarding, cybersecurity and acceptable-use requirements and applicable UAE legislation.
- Access to websites, applications, services, or types of online content may be restricted to protect students, maintain network security and ensure sufficient connectivity for teaching and learning.

Access to the school network is a privilege and may be restricted, suspended or withdrawn where a device or user presents a safeguarding, security or operational risk.

Authentication and Account Security

Students must:

- use only their own school-issued account and network credentials;
- keep passwords, authentication codes and other login information private;
- never use another person's account or permit another person to use their account;
- use multi-factor authentication where required by the school;
- log out of shared applications and services when they are no longer in use; and
- report suspected account compromise, unauthorized access or disclosure of login credentials immediately.
- Students must not share passwords with friends or other students. Younger students may receive age-appropriate assistance from their parents or guardians in managing their devices and accounts.

Device Security Requirements

Before a personal device is permitted to connect to the school network, it must:

- meet the current Madar BYOD Minimum Device Specifications;
- use a supported and appropriately licensed operating system;
- have current operating-system, browser and application security updates installed;
- use an appropriate device passcode, password or biometric lock;
- have antivirus or other endpoint-security protection enabled where required for the device type;
- be free from known malware, unauthorized software or configurations that could compromise the school network; and
- accept any school-approved network certificate, security profile or connectivity configuration required to provide secure access.
- Students and parents or guardians must not remove or interfere with school-required network certificates, security settings or profiles while the device is authorized to access school systems.
- The school may deny or remove network access until identified security or compatibility concerns have been addressed.

Prohibited Connectivity and Security Practices

Students must not:

- use a virtual private network (VPN), proxy service, anonymizing browser, alternative DNS service or similar technology to bypass the school's filtering, monitoring or security controls;
- use personal hotspots or tethering to provide unfiltered internet access to themselves or others;
- attempt to disable, evade or interfere with network filtering, monitoring, authentication or security measures;
- scan, probe, test or interfere with the school network, connected devices, accounts or systems;
- alter or disguise a device's identity or network information to evade restrictions;
- connect unauthorized networking equipment, storage devices or other hardware to school systems;
- attempt to access restricted files, accounts, systems or administrative functions; or
- introduce malware, malicious code or any software intended to disrupt, damage or obtain unauthorized access.
- Security testing may only be undertaken as part of an expressly authorized and supervised educational activity.

Filtering, Monitoring and Privacy

When a personal device connects to the school network or accesses a school-provided account, platform or digital service, the school may collect and review relevant information, including:

- the identity of the user and device;
- connection dates, times and duration;
- websites, services and applications accessed through the school network;
- network traffic and security alerts;
- school-account activity; and information reasonably required to investigate safeguarding, cybersecurity, academic-integrity or acceptable-use concerns.

Monitoring will be undertaken for legitimate educational, safeguarding, security, operational and legal purposes. Students should not expect activity conducted through the school network, school accounts or school-managed platforms to be private.

Routine network monitoring does not give the school unrestricted access to personal photographs, messages, files or accounts stored on a privately owned device. Where examination of a device may be necessary in response to a specific concern, this will be managed in accordance with applicable law and the school's safeguarding, behavior-management and investigation procedures.

Reporting Concerns

Students must immediately report:

- suspected loss, theft or compromise of a device or school account;
- suspicious login notifications or unexpected authentication requests;
- malware, unusual device behavior or suspected security breaches;
- accidental access to inappropriate, harmful, or illegal content;
- cyberbullying, threatening communication or other online-safety concerns; and
- any attempt by another person to obtain their password or access their device.

Technical and account-security concerns should be reported to a teacher or the IT Department. Safeguarding concerns should be reported immediately to a trusted member of staff or the school's designated safeguarding personnel.

Students will not be penalized for promptly reporting accidental access to inappropriate content or a genuine security concern, provided they did not deliberately seek, save, share or continue accessing the material.

IT Support

The IT Department will provide reasonable support for:

- connecting approved devices to the Student BYOD Wi-Fi network;
- installing or checking required network certificates, security profiles and connectivity settings;
- accessing school-issued accounts, Toddle and other approved digital platforms;
- diagnosing school-network or school-account access problems; and
- identifying whether a device meets the school's minimum connectivity and security requirements.

The school does not provide routine support for:

- repairing, servicing or upgrading personal devices;
- replacing damaged or missing hardware;
- recovering personal files or data;
- resolving problems with privately purchased software, warranties or subscriptions; or
- configuring personal accounts and services unrelated to school learning.

Where a device requires repair or specialist technical support, responsibility remains with the student's parent or guardian and the relevant retailer, manufacturer, or service provider.

6. Student Responsibilities

All students participating in the Madar International School BYOD programme must use their devices in ways that support learning, demonstrate the school's core values and comply with this policy and all related school policies.

These responsibilities apply whenever a personal device is brought onto school premises, connected to school systems, or used for a school-related activity.

Daily Readiness

Students must:

- bring their approved personal learning device to school each day unless instructed otherwise by a member of staff;
- ensure that the device is fully charged at the beginning of the school day;
- bring any required accessories, including headphones, keyboard, stylus or charger, where applicable;
- ensure that the device is functioning properly and ready for learning;
- access Toddle and other required learning platforms using their school-issued account; and
- follow established classroom procedures for taking out, using and storing devices.

Charging facilities may be limited. Students must not use charging cables or adapters in ways that create a safety hazard or disrupt teaching and learning.

Learning and Classroom Use

Students must:

- use their device only when directed or permitted by a member of staff;
- use the device for the learning activity or purpose identified by the teacher;
- close or put away the device immediately when instructed;
- remain focused on the assigned platform, application or task;
- bring the device to assessments where its use has been authorised;
- follow teachers' instructions regarding the use of cameras, microphones, headphones, messaging and artificial intelligence; and
- balance device use with handwriting, discussion, practical activities, physical activity and face-to-face interaction as directed by staff.

Having a device at school does not give a student permission to use it at any time or for any purpose.

Required Applications, Updates and Security

Students must:

- ensure that all school-required applications, software and security configurations remain installed and operational;
- keep the device's operating system, browser and applications updated;
- use an appropriate passcode, password or biometric lock;
- keep school login credentials and authentication codes private;
- use only their own school-issued accounts;
- preserve any school-required network certificates, security profiles or settings; and
- comply promptly with reasonable instructions from authorized school or IT staff where a device presents compatibility, safeguarding or security concern.

Students must not install, retain or use applications, files or configurations that are unlawful, inappropriate, malicious, or intended to bypass school controls.

Safe and Responsible Use

Students must:

- communicate respectfully and demonstrate Madar's core values in all digital interactions;
- protect their own personal information and respect the privacy of others;
- respect copyright, intellectual property and academic-integrity requirements;
- use artificial intelligence only where permitted and acknowledge its use as required;
- avoid accessing, creating, storing or sharing harmful, offensive, discriminatory, violent, or otherwise inappropriate content;

- never use a device to bully, threaten, harass, impersonate, embarrass or exclude another person; and
- report inappropriate content, unsafe communication, cyberbullying, or other digital-safeguarding concerns immediately.

Safe Handling and Physical Security

Students must:

- clearly label the device and its protective case with their name and grade or class;
- transport and store the device in an appropriate protective case, sleeve or bag;
- handle their own device and the devices of others carefully;
- keep food and liquids away from devices;
- store the device securely when it is not in use;
- never leave the device unattended in an unsecured location; and
- follow staff instructions regarding secure storage during physical education, assemblies, examinations, trips and other activities.

Students must not lend their device to another student or use another student's device without express permission from both the device owner and a member of staff.

Loss, Damage or Theft

Students must:

- take reasonable care of their device and accessories;
- report loss, damage or suspected theft immediately to a member of staff;
- report any damage caused to another person's device honestly and promptly;
- provide accurate information when the school investigates an incident; and
- inform a teacher as soon as possible if device unavailability may affect their learning.

Students must not attempt to repair damaged electrical components, batteries, plugs, or charging cables while at school.

Reporting Technical or Security Concerns

Students must promptly report:

- difficulty accessing the school network, Toddle or another required platform;
- a lost or compromised password;
- suspicious messages, login notifications or authentication requests;
- suspected malware or unusual device behavior;
- accidental access to inappropriate or harmful content; or
- any attempt to bypass the school's filtering, monitoring or security controls.

Concerns should be reported to a teacher, the IT Department or designated safeguarding personnel, depending on their nature.

7. Parent and Guardian Responsibilities

Parents and guardians are essential partners in supporting the safe and effective implementation of the Madar International School BYOD programme. They are responsible for providing and maintaining an appropriate device and reinforcing responsible technology use at home.

Providing an Approved Device

Parents and guardians must:

- provide a device appropriate to the student's grade level and compliant with the current Madar BYOD Minimum Device Specifications;
- ensure that the device and required accessories are available by the date communicated by the school;
- provide an appropriate protective case, sleeve or bag;
- provide headphones with a microphone and any required keyboard, charger or other accessories;
- clearly label the device and accessories with the student's name and grade or class; and
- ensure that the device is safe, functional and suitable for daily school use.

Parents and guardians should consult the school before purchasing a device where they are uncertain about its suitability or compatibility.

Maintenance, Software and Security

Parents and guardians must:

- arrange the installation of school-required applications, software and connectivity settings;
- ensure that the operating system, browser, applications and security software remain supported and updated;
- ensure that the device is protected by an appropriate passcode, password or biometric lock;
- maintain any school-required network certificates, security profiles or configurations;
- ensure that age-appropriate parental controls and privacy settings are applied where appropriate;
- arrange regular backup of schoolwork and other important files; and
- ensure that the device does not contain unlawful, age-inappropriate or malicious applications or content.

Where the school requires a security profile, certificate or device-management configuration, parents and guardians must review the information provided and complete any required consent or enrolment process before the device is connected to school systems.

Supporting Responsible and Safe Use

Parents and guardians are expected to:

- read and discuss this policy and the Acceptable Use Agreement with their child;
- reinforce expectations for respectful communication, digital citizenship, academic integrity, online safety and responsible AI use;
- establish age-appropriate routines and boundaries for technology use at home;
- monitor their child's use of the device and online services in a proportionate and age-appropriate manner;
- encourage balanced use of technology, including appropriate sleep, physical activity and time away from screens;
- support their child in protecting passwords, personal information and digital accounts;
- encourage their child to report harmful content, unsafe contact, cyberbullying or other online concerns; and
- contact the school promptly where they become aware of a safeguarding, behavioral or security concern connected with school-related technology use.

Daily Readiness and Attendance

Parents and guardians should support their child in:

- bringing the approved device to school each day;
- charging it fully before the beginning of the school day;
- bringing all required accessories;
- storing and transporting it safely; and
- developing increasing independence in managing the device according to the student's age and stage of development.

Repairs, Replacement, and Insurance

Parents and guardians are responsible for:

- the maintenance, repair and replacement of their child's personal device and accessories;
- arranging repairs promptly to minimize disruption to learning;
- informing the school when the device will be unavailable for an extended period;
- protecting the device against loss, theft and accidental damage; and
- meeting costs associated with warranties, insurance, repairs or replacement.

Accidental-damage, loss and theft insurance or an appropriate extended warranty is strongly recommended.

The school will take reasonable measures to promote secure device use and storage. However, personal devices remain the property and responsibility of the student and their parent or guardian.

Loss or Theft

If a device is lost or stolen, parents and guardians must:

- notify the school as soon as possible;
- take appropriate steps to secure the device and associated accounts, including changing passwords or using remote-locking features;
- report suspected theft to the police where appropriate; and
- provide the school with relevant information required to investigate an incident occurring on school premises or during a school activity.

Temporary Device Unavailability

Where a device is unavailable because of repair, loss or another genuine difficulty, parents or guardians must inform the school promptly.

Any temporary school device, where available, will be issued subject to the school's lending procedures, availability and any applicable agreement. The school cannot guarantee that a loan device will always be available.

Acknowledgement and Consent

Parents and guardians must:

- review this policy and the associated Parent and Student BYOD and Acceptable Use Agreement;
- ensure that their child understands the expectations appropriate to their age;
- complete the required acknowledgement or consent process before the device is connected to school systems; and
- notify the school of any change affecting the student's device, access needs or ability to comply with the programme requirements.

Acknowledgement will normally be completed at the beginning of each academic year and whenever the policy or associated requirements are materially updated.

Failure to meet the BYOD requirements may result in the device being refused access to the school network or other proportionate measures being applied in accordance with relevant school policies.

8. School Responsibilities

Madar International School is responsible for establishing and maintaining the educational, technical and safeguarding arrangements required to support the effective implementation of the BYOD programme. The school will take reasonable and proportionate measures to provide a safe, secure, inclusive and purposeful digital learning environment.

Teaching and Learning

The school will:

- ensure that personal devices are used purposefully to support curriculum objectives and student learning;
- provide students with access to Toddle and other school-approved learning platforms, applications and digital resources;
- establish age-appropriate expectations for device use across Grades 1–12;
- ensure that teachers determine when and how devices are used during lessons;
- promote a balanced approach that includes discussion, handwriting, practical learning, physical activity and face-to-face interaction;
- provide alternatives where the use of a device is not educationally appropriate or where a reasonable adjustment is required; and
- regularly evaluate the effect of technology use on teaching quality, student engagement, progress and wellbeing.

Access to a device does not mean that it will be used continuously throughout every lesson or school day.

Staff Training and Guidance

The school will:

- provide teachers and relevant staff with guidance and professional development on the effective use of Toddle, digital tools and personal devices;
- support staff in teaching digital citizenship, online safety, information literacy and responsible AI use;
- provide clear classroom-management procedures for the use and storage of devices;
- ensure that staff understand how to identify and report safeguarding, behavioral, academic-integrity and cybersecurity concerns; and
- communicate changes to BYOD requirements, approved platforms and school procedures.

Network Access and Cybersecurity

The school will take reasonable measures to:

- provide a designated Student BYOD Wi-Fi network;
- maintain appropriate network security, authentication and access controls;
- filter and monitor internet activity conducted through the school network in accordance with safeguarding requirements and applicable UAE legislation;
- protect school systems, accounts and data from unauthorised access;
- restrict access to websites, applications or services that present a safeguarding, cybersecurity, legal or operational risk;

- investigate suspected misuse, security incidents and attempts to bypass school controls; and
- restrict or remove network access where a device or user presents a security, safeguarding or operational risk.

Filtering and monitoring systems reduce risk but cannot guarantee that all harmful or inappropriate content will be prevented. Students and staff remain responsible for reporting any inappropriate content or online-safety concern promptly.

Student Accounts and Digital Platforms

The school will:

- provide students with appropriate school-issued accounts and access credentials;
- establish age-appropriate permissions for Toddle and other approved digital platforms;
- apply appropriate privacy and security settings to school-managed accounts;
- provide guidance on passwords, authentication and account security;
- respond to suspected account compromise or unauthorized access;
- manage student access when a student joins, changes grade level or leaves the school; and
- communicate relevant platform terms, privacy information or consent requirements to parents and guardians.

Digital Safeguarding and Student Wellbeing

The school will:

- teach and reinforce safe, respectful and responsible digital behavior;
- provide students with clear ways to report harmful content, cyberbullying, unsafe contact or other concerns;
- respond to digital-safeguarding concerns in accordance with the Child Protection and Safeguarding Policy;
- consider students' ages, developmental needs and vulnerabilities when determining appropriate technology use;
- promote healthy and balanced use of devices; and
- work with parents and guardians where concerns arise about a student's online safety, behavior or wellbeing.

Academic Integrity and Responsible AI Use

The school will:

- establish clear expectations for authentic student work and the acknowledgement of sources;
- explain when collaboration, online assistance and artificial intelligence may or may not be used;

- teach students how to use digital information and artificial intelligence critically, safely, ethically and responsibly;
- require students to acknowledge or reference AI assistance where appropriate;
- design and supervise assessments in ways that support academic integrity; and
- respond to suspected misuse in accordance with the Academic Integrity Policy and Behavior Management Policy.

Inclusion and Equitable Access

The school will:

- work with families where access to a suitable device presents a genuine difficulty;
- consider reasonable adjustments, alternative devices or assistive technologies for students with identified learning, accessibility or medical needs;
- involve the Inclusion Team, relevant staff and parents or guardians when determining appropriate adjustments;
- take reasonable steps to ensure that temporary device unavailability does not unnecessarily prevent a student from participating in learning; and
- provide access to a school-owned loan device where appropriate and available, subject to the school's lending procedures.

The availability of loan devices cannot be guaranteed. Any school-owned device issued temporarily remains subject to the school's device-lending conditions and acceptable-use requirements.

Technical Support

The IT Department will provide reasonable support for:

- confirming whether a device meets the published minimum requirements;
- connecting approved devices to the Student BYOD Wi-Fi network;
- configuring required network certificates or connectivity settings;
- accessing school-issued accounts, Toddle and other approved platforms;
- diagnosing basic school-network and school-account access problems; and
- identifying security or compatibility issues affecting access to school systems.

The school is not responsible for:

- repairing, servicing or upgrading personally owned devices;
 - replacing lost, stolen or damaged devices or accessories;
 - recovering personal data or files;
 - resolving warranty, insurance or retailer disputes;
 - supporting personal applications, accounts or subscriptions unrelated to school learning;
- or

- guaranteeing that every personally owned device or application will remain compatible with school systems.

Monitoring, Investigation and Privacy

The school will:

- monitor activity conducted through the school network, school-issued accounts and school-managed platforms for legitimate educational, safeguarding, security and operational purposes;
- limit access to monitoring information to authorized personnel;
- handle information collected through monitoring in accordance with applicable school procedures and legal requirements;
- investigate suspected breaches fairly and proportionately; and
- involve parents, safeguarding personnel or external authorities where required by the nature of an incident.

The school will not conduct unrestricted or routine searches of students' personal photographs, messages, accounts or files. Where access to information on a personal device is reasonably required in response to a specific concern, it will be managed through an authorized process consistent with applicable law and the school's safeguarding, behavior and investigation procedures.

Device Safety and Storage

The school will:

- establish appropriate procedures for the use and storage of devices during lessons and school activities;
- identify secure storage arrangements where reasonably practicable;
- require students to follow staff instructions concerning devices during physical education, assemblies, assessments, trips and other activities;
- respond to reported incidents of loss, theft or damage occurring at school; and
- take reasonable steps to investigate relevant incidents.

Personal devices remain the property and responsibility of students and their parents or guardians.

Behavior and Policy Compliance

The school will:

- communicate BYOD expectations clearly to students, parents, guardians and staff;
- apply expectations consistently and in an age-appropriate manner;
- respond to breaches in accordance with the Behaviour Management Policy and other relevant policies;

- consider the seriousness, context and impact of an incident, including any safeguarding or additional learning needs;
- use education, support and restorative intervention where appropriate; and
- restrict device, network or platform access where this is necessary to protect learning, safety or security.

Removal of access should be proportionate and, wherever possible, should not unnecessarily prevent the student from continuing their education.

9. Acceptable Use Guidelines

Madar International School recognizes the educational value of personal learning devices while promoting safe, purposeful and balanced technology use.

These guidelines are intended to:

- support effective teaching and learning;
- protect instructional time and students' concentration;
- reduce distraction and inappropriate or excessive use;
- protect students, school systems and information;
- promote academic integrity and responsible use of artificial intelligence; and
- develop respectful, responsible and critically aware digital citizens.

Use of a personal device at school and access to the school's network, accounts and digital services are conditional upon compliance with this policy. Students must demonstrate the school's values of respect, compassion, mercy, belonging, tolerance, kindness, collaboration, leadership, and global understanding in all digital interactions.

These expectations apply whenever a personal device is used on school premises, connected to school systems or used for a school-related activity.

Educational Use

Students must:

- use their device only when directed or permitted by a member of staff;
- use the device for the learning activity identified by the teacher;
- access only the websites, applications, files and digital resources required or approved for the activity;
- remain focused on the assigned task;
- use school-issued accounts when accessing Toddle and other school platforms;
- stop using, close or store the device immediately when instructed; and

- follow all classroom, assessment and examination procedures relating to device use.

Personal activities including private messaging, social media, online shopping, gaming, entertainment and non-educational browsing are not permitted during the school day unless expressly authorized by a member of staff for a specific educational purpose.

Classroom Focus and Balanced Use

Students must:

- keep notifications disabled or use an appropriate focus mode during lessons;
- keep the device screen visible to the supervising member of staff when requested;
- avoid switching between unrelated applications, websites or accounts;
- close the device or turn the screen face down when directed;
- participate fully in discussion, handwriting, practical work, physical activity and face-to-face collaboration; and
- respect device-free lessons, activities, spaces and periods established by the school.

Teachers determine when personal devices should and should not be used. Students must not assume that every learning activity requires a device.

Sound, Headphones, Cameras and Microphones

Students must:

- keep the device muted unless sound is required and authorized by a member of staff;
- use headphones only when directed or permitted;
- keep headphone volume at a safe level that allows them to hear staff instructions;
- obtain permission before activating a camera or microphone; and
- stop recording or capturing images immediately when instructed.

Students must not photograph, film, livestream or make an audio recording of another student, member of staff or visitor.

Images, audio, or video recorded for an authorized school activity must not be published, forwarded or uploaded to personal accounts or public platforms without school approval and the appropriate consent.

Respectful Communication and Digital Citizenship

Students must:

- communicate respectfully, honestly and responsibly;
- use language and content appropriate to the student's age and the school environment;
- respect different identities, cultures, beliefs, opinions and backgrounds;
- protect their own privacy and the privacy of others;

- obtain permission before sharing another person's image, work or personal information;
- respect copyright, intellectual property and licensing requirements; and
- acknowledge information, images, media and ideas taken from other sources.

Students must not use technology to:

- bully, threaten, harass, intimidate or exclude another person;
- discriminate against or insult another person or group;
- impersonate another person or misrepresent their identity;
- spread rumors or knowingly false or misleading information;
- embarrass, ridicule or damage another person's reputation;
- create, manipulate or distribute deceptive images, audio or video; or
- communicate with others in a way that compromises safety or wellbeing.

These expectations apply to school-related digital conduct both on and off school premises where it affects a student, member of staff, the school community or the safe operation of the school.

Privacy and Personal Information

Students must:

- keep passwords, authentication codes and account-recovery information private;
- use only their own accounts and authorized profiles;
- protect personal details such as addresses, telephone numbers, identification information and live location;
- review privacy and sharing settings before publishing or submitting information;
- avoid sharing confidential school information; and
- report any request for personal information, images, passwords or private communication that causes concern.

Students must not access, copy, alter, delete or share another person's files, accounts, messages or personal information without authorization.

Academic Integrity

Students must use their devices in accordance with the school's Academic Integrity Policy.

Students must:

- submit work that accurately represents their own knowledge, understanding and effort;
- acknowledge and reference sources as required;
- follow instructions concerning collaboration, research assistance and permitted resources;
- keep assessment materials and responses secure;
- avoid giving or receiving unauthorized assistance; and
- explain or demonstrate their learning when requested.

Students must not use a device to:

- plagiarize or submit another person's work as their own;
- access unauthorized information during an assessment;
- photograph, copy, store or distribute confidential assessment materials;
- communicate with another person during an assessment without permission; or
- assist another student in breaching academic-integrity requirements.

Responsible Use of Artificial Intelligence

Artificial intelligence may be used only when permitted by the teacher and in accordance with the Academic Integrity Policy and the instructions for the activity or assessment.

When AI use is permitted, students must:

- use school-approved tools and accounts where required;
- protect personal, sensitive and confidential information;
- critically evaluate AI-generated information for accuracy, bias and suitability;
- check claims against reliable sources;
- revise and take responsibility for any AI-assisted work they submit;
- acknowledge or describe AI assistance in the manner required by the teacher; and
- be able to explain the ideas, decisions and learning represented in their work.

Students must not use AI to:

- complete work that they are expected to produce independently;
- conceal the extent of AI assistance;
- fabricate evidence, references, research findings or data;
- impersonate another person;
- create deceptive or harmful images, audio, video or messages;
- make significant decisions about another person; or
- upload personal, confidential or copyrighted school information without authorization.

Appropriate Content

Students must not use a device to access, create, download, store, display or share content that is:

- unlawful or contrary to applicable UAE requirements;
- sexually explicit or pornographic;
- abusive, discriminatory, hateful or harassing;
- excessively violent or intended to glorify violence;
- extremist or supportive of unlawful organizations or activity;
- related to self-harm, suicide or dangerous behavior in a manner that promotes harm;
- defamatory, threatening or deliberately humiliating;

- malicious, deceptive or intended to cause disruption; or
- otherwise inappropriate for the student's age or a school environment.

Students who accidentally encounter inappropriate or harmful content must close or minimize it where safe to do so and report it immediately. They must not save, forward or show the material to other students.

Personal Content on Learning Devices

Devices brought to school under the BYOD programme are intended primarily for learning. Students and parents or guardians must ensure that devices do not contain unnecessary personal content, including personal photographs, videos, private messages or sensitive information.

Copyright and File Sharing

Students must:

- use legally obtained software, media and digital resources;
- comply with applicable licenses and terms of use;
- obtain permission before reproducing or distributing another person's work; and
- provide appropriate acknowledgement or attribution.

Students must not:

- download or distribute pirated software, films, music, books, games or other copyrighted material;
- use unauthorised peer-to-peer or file-sharing services;
- copy licensed school resources for personal distribution; or
- use school systems to conduct unlawful downloading or sharing.

Network and System Use

Students must:

- connect only to the designated Student BYOD Wi-Fi network;
- use their own authorised school credentials;
- comply with school filtering, monitoring and security controls;
- keep required security settings and updates active; and
- report suspected security concerns promptly.

Students must not:

- use personal hotspots, tethering or mobile data unless expressly authorized;
- use VPNs, proxies, alternative DNS services or other tools to bypass school controls;
- attempt to gain unauthorized access to accounts, devices, files, networks or systems;
- interfere with filtering, monitoring, authentication or cybersecurity controls;

- introduce malware or disruptive software;
- scan, probe or test the school network without formal authorization; or
- knowingly consume excessive network capacity in a way that affects other users.

Applications and Software

Because the device is personally owned, the school will not routinely control all applications installed for use outside school. However, students must not open or use at school any application, game, file, account or service that:

- is inappropriate for their age or the school environment;
- distracts from learning;
- creates a safeguarding or cybersecurity risk;
- bypasses school controls;
- enables unauthorized communication, recording or file sharing; or
- breaches this policy or another school requirement.

The school may require an application or configuration to be removed, disabled or not used at school where it presents a security, safeguarding, compatibility or educational concern.

Reporting and Cooperation

Students must promptly report:

- harmful or inappropriate content;
- cyberbullying, harassment or threatening communication;
- loss or compromise of a device or account;
- suspected malware or unauthorized access;
- requests for passwords, personal information or inappropriate images;
- accidental breaches of this policy; and
- attempts by another person to bypass school controls.

Reports may be made to a teacher, the IT Department or designated safeguarding personnel, depending on the nature of the concern.

Compliance and Consequences

Failure to comply with these guidelines may result in one or more of the following:

- an instruction to stop using or store the device;
- removal of the device from the immediate learning activity;
- temporary restriction or withdrawal of network, account or platform access;
- confiscation and parent or guardian collection in accordance with school procedures;
- completion of educational, restorative or safeguarding interventions;

- application of consequences under the Behavior Management or Academic Integrity Policy; and/or
- referral to safeguarding personnel, senior leaders or relevant external authorities where required.

Responses will be proportionate and will take account of the student's age, intent, the seriousness and impact of the incident, previous concerns, safeguarding considerations, and any identified additional needs.

10. Acceptable Use: Digital Wellbeing

Madar International School recognizes the educational value of personal learning devices while promoting healthy, balanced and age-appropriate technology habits.

The school's approach to digital wellbeing is intended to:

- maintain students' attention and engagement in learning;
- balance digital activities with handwriting, reading, discussion, practical learning, movement and face-to-face interaction;
- reduce unnecessary distraction and excessive or compulsive device use;
- support healthy sleep, posture, vision and physical activity;
- help students recognize and manage the effect of technology on their emotions, relationships and wellbeing; and
- develop increasing independence, self-regulation and responsible decision-making.

These expectations apply whenever personal devices are used on school premises or during school-related activities.

Purposeful Device Use

Students must:

- use their device only when directed or permitted by a member of staff;
- use the device for the learning activity identified by the teacher;
- stop using, close or store the device immediately when instructed;
- remain on the assigned application, website or learning platform;
- avoid unnecessary switching between applications or tasks; and
- participate fully in non-digital activities when required.

Teachers will determine whether a digital or non-digital approach is most appropriate for each learning activity.

Focus Mode and Notification Management

During lessons and other supervised activities, students must:

- enable Do Not Disturb, focus mode or an equivalent setting when instructed;
- disable or mute non-essential notifications;
- close personal messaging, social-media, gaming and entertainment applications;

- keep sound muted unless audio is required for learning; and
- ensure that alerts, calls or notifications do not disrupt teaching, learning or other school activities.

Parents and guardians should avoid contacting students directly through their personal learning devices during the school day. Urgent messages should be communicated through the school's established contact procedures.

Device-Free Times and Spaces

Unless a member of staff has expressly authorized device use for a supervised educational or school activity, personal learning devices must be switched off, closed or securely stored during:

- registration or homeroom;
- assemblies;
- break and lunchtime;
- unstructured social time;
- physical education and sporting activities;
- performances, ceremonies and formal school events; and
- any lesson, activity, location or period designated as device-free.

Devices must never be used in:

- toilets or bathrooms;
- changing rooms;
- prayer areas during prayer or reflection;
- medical or counselling spaces without permission; or
- any other location where their use could compromise privacy, dignity or safety.

The school may establish additional device-free periods or areas to support students' concentration, social interaction, safeguarding, and wellbeing.

Balanced Learning and Screen Breaks

The school will promote an appropriate balance between digital and non-digital learning.

Teachers will:

- use technology where it adds clear educational value;
- incorporate discussion, handwriting, reading, practical work, collaboration and physical movement into learning;
- provide reasonable opportunities for students to look away from screens, change posture and move during extended periods of device use;
- avoid requiring students to remain continuously engaged with a screen for an entire lesson where this is not educationally necessary; and

- consider students' ages, developmental stages, accessibility needs and the nature of the activity when planning device use.

In Elementary School, device use will normally take place through shorter, clearly structured and teacher-directed activities. As students progress through Middle and High School, they will be expected to demonstrate increasing independence in managing their attention, notifications and screen use.

Social and Emotional Wellbeing

Students must not allow device use to interfere unnecessarily with:

- face-to-face communication;
- participation in lessons and school activities;
- friendships and positive social interaction;
- physical activity;
- rest and sleep; or
- their own emotional wellbeing or that of others.

Students are encouraged to seek help if online activity causes them to feel anxious, distressed, pressured, excluded, distracted or unable to stop using a particular application or service.

Students must report cyberbullying, harmful content, unsafe contact, social pressure or other online experiences that affect their wellbeing to a trusted member of staff.

Digital Wellbeing Education

The school will provide age-appropriate learning and guidance on:

- healthy and balanced technology use;
- managing notifications, distractions and digital habits;
- recognizing persuasive and attention-capturing design;
- understanding the effect of screen use on sleep, concentration and mood;
- managing social-media pressure and online comparison;
- responding to cyberbullying and harmful online interactions;
- maintaining privacy and healthy digital boundaries;
- evaluating personal patterns of device use; and
- knowing when and how to seek help.

Students will be encouraged to reflect on their digital habits and develop practical strategies for maintaining focus, balance and wellbeing.

Additional and Individual Needs

The school recognizes that some students may need to use a device during a normally device-free period because of an identified learning, accessibility, communication or medical need.

Appropriate adjustments will be agreed with the student, parent or guardian, Inclusion Team and relevant school staff. Students will not be disadvantaged for using approved assistive technology or an agreed digital support.

Support and Response to Concerns

Where a student does not meet the school's digital-wellbeing expectations, staff will normally use an age-appropriate and graduated response, which may include:

- a reminder or redirection;
- an instruction to close or store the device;
- a restorative conversation and review of expectations;
- temporary restriction of device use within a lesson or activity;
- communication with the student's parent or guardian;
- an agreed device-use or wellbeing support plan; and/or
- referral to the Inclusion, pastoral, counselling or safeguarding team where appropriate.

Repeated or serious breaches may result in temporary restriction of BYOD privileges or other proportionate action under the Behavior Management Policy.

11. Monitoring, Prohibited Use and Consequences

Monitoring

- Activity conducted through the Student BYOD Wi-Fi, school-issued accounts and school-managed platforms may be filtered, logged and monitored for educational, safeguarding, cybersecurity and operational purposes.
- Monitoring will be conducted by authorized personnel in accordance with applicable UAE law, ADEK requirements and school policies. Students should not expect privacy when using the school network or school-managed services.

Where there is a specific and reasonable concern involving safeguarding, serious misconduct, cybersecurity, unlawful activity or a breach of this policy, an authorized member of staff may require limited access to relevant content or applications on a device.

Any inspection will:

- have a clear and documented purpose;
- be limited to information relevant to the concern;
- respect the student's privacy and dignity;
- be conducted in accordance with school safeguarding and investigation procedures; and
- involve the parent or guardian where appropriate.

Students must cooperate with reasonable instructions. Where access to a personal device is required, the school should normally ask the student to navigate to the relevant content rather

than require passwords to be disclosed. Serious concerns may be referred to the parent or guardian, ADEK, Abu Dhabi Police or another appropriate authority.

Confiscation and Secure Storage

A device may be confiscated temporarily where its use:

- disrupts teaching or learning;
- breaches this policy or the Acceptable Use Guidelines;
- presents a safeguarding or cybersecurity risk; or
- is relevant to a serious disciplinary or safeguarding concern.

The student will be informed why the device has been confiscated. The device will be switched off or secured, recorded and stored safely. It may be returned to the student or released to a parent or guardian, depending on the circumstances and school procedures.

Consequences

Breaches will be addressed proportionately under the Behavior Management Policy, Acceptable Use Agreement, and other relevant school policies. Actions may include:

- a warning, restorative conversation or educational intervention;
- temporary removal of the device from a lesson or activity;
- parent or guardian contact;
- temporary restriction of network, account or BYOD access;
- confiscation and parent or guardian collection;
- additional disciplinary or safeguarding action; and/or
- referral to ADEK, Abu Dhabi Police or another appropriate authority where required.

Consequences will take account of the student's age, intent, the seriousness and impact of the incident, previous concerns and any safeguarding or additional learning needs. Permanent withdrawal of access should be exceptional and must not unnecessarily prevent the student from continuing essential learning.

Misuse and Disciplinary Action

Misuse of personal devices will be classified and addressed through the behavior levels established in the Madar International School Behavior Management Policy. Consequences will be proportionate to the student's age, intent, the seriousness and impact of the incident, previous behavior and any safeguarding or additional learning needs.

Level 3 Behaviors: Significant or Repeated Misuse

Level 3 behaviors may include:

- repeated use of a device without permission;
- repeated gaming, messaging, social-media use, streaming or non-educational browsing during lessons;

- persistent refusal to close or store a device when instructed;
- repeated disruption of teaching and learning through device use;
- accessing unapproved websites, applications or accounts;
- using personal hotspots or mobile data without permission;
- taking photographs, video or audio recordings;
- sharing another person's image, work or personal information without consent;
- using inappropriate, offensive or disrespectful language online;
- using another person's account or allowing another person to use a school account;
- using AI or online resources contrary to teacher or assessment instructions; or
- refusing to cooperate with a reasonable and authorized investigation.

Possible Level 3 consequences may include:

- a formal warning and restorative conversation;
- confiscation of the device for the remainder of the lesson or school day;
- parent or guardian contact;
- parent or guardian collection of the device;
- formal recording of the incident;
- completion of a reflection or digital-citizenship intervention;
- a device-use or behavior support plan;
- temporary restriction of BYOD, network or platform access; and/or
- further action permitted under the Behavior Management or Academic Integrity Policy.
- Repeated Level 3 behavior may be escalated to Level 4.

Level 4 Behaviors: Serious Misuse

Level 4 behaviors may include:

- repeated Level 3 offences;
- cyberbullying, harassment, threats, discrimination or intimidation;
- creating, accessing, possessing or sharing sexually explicit, violent, extremist, hateful, unlawful or seriously harmful content;
- recording another person in circumstances that compromise privacy, dignity or safety;
- distributing images, video or audio without permission;
- deliberately bypassing filtering, monitoring or security controls using a VPN, proxy, hotspot or another method;
- attempting to gain unauthorized access to accounts, devices, files, networks or school systems;
- introducing malware or deliberately damaging or disrupting systems;
- stealing passwords, impersonating another person or using a false identity to cause harm;

- using a device to cheat, distribute confidential assessment materials or commit a serious academic-integrity breach;
- fraud, phishing or another unlawful online activity;
- using technology in connection with a serious safeguarding concern; or
- concealing, deleting or distributing evidence relating to a serious incident.

Possible Level 4 consequences include:

- immediate confiscation and secure storage of the device;
- immediate parent or guardian notification and collection;
- a formal parent–school leadership meeting;
- suspension of BYOD, network, account or platform access for a defined period;
- a formal written warning issued and recorded in accordance with school and ADEK procedures;
- safeguarding intervention;
- an individual risk assessment, behavior contract or reintegration plan;
- suspension or another sanction permitted under the approved Behavior Management Policy; and/or
- referral to ADEK, Abu Dhabi Police or another appropriate authority where required.

Level 4 incidents may proceed directly to formal disciplinary, safeguarding or legal action without applying lower-level consequences first.

Confiscation and Restoration of Access

When a device is confiscated, the reason and duration will be recorded and the device will be stored securely. Depending on the seriousness of the incident, it may be returned to the student or released only to a parent or guardian.

Restoration of BYOD or network access may require:

- completion of the assigned consequence or intervention;
- a meeting with the student and parent or guardian;
- evidence that the student understands the breach and its impact;
- agreement to follow a behavior or device-use support plan; and
- confirmation that any safeguarding or cybersecurity risk has been addressed.
- Permanent withdrawal of BYOD access should be reserved for serious or continuing risk and authorized by school leadership. The school will ensure that any restriction does not unnecessarily prevent the student from accessing essential learning.

12. Agreement and Acknowledgement

Participation in the Madar International School BYOD programme is conditional upon completion of the electronic BYOD Agreement and Acknowledgement Form by the student's parent or guardian.

By submitting the form, the parent or guardian confirms that:

- they have read and understood the BYOD Policy with their child;
- they agree to support their child's compliance with the policy;
- the student understands and accepts their responsibilities;
- the device meets the school's minimum technical requirements;
- they consent to the device being enrolled for access to the school's network and approved digital services; and
- the information provided in the form is accurate.
- Electronic submission will be treated as the parent or guardian's formal acknowledgement and consent.

Device Enrolment Consent

The parent or guardian authorizes the school to enroll the nominated device in the BYOD programme. Enrolment may include:

- registering the student and device;
- recording necessary device information, such as device type, operating system and device identifier;
- configuring access to the Student BYOD Wi-Fi;
- installing or requiring approved applications, certificates, profiles or security settings necessary for school use;
- checking whether the device meets minimum security and compatibility requirements; and
- restricting or removing access where the device no longer meets requirements or presents a security, safeguarding or operational risk.

Device enrolment does not give the school routine access to personal photographs, videos, messages or other private content. Any access required in response to a specific concern will follow the inspection provisions of this policy.

Parents and students must not remove, disable or interfere with required school configurations while the device remains enrolled. Enrolment and school access may be removed when the student leaves the school, changes device or withdraws from the BYOD programme.

Parent or Guardian Commitment

As the parent or guardian, I agree to:

- provide and maintain a device that meets the school's minimum specifications;
- ensure that the device is updated, secure and suitable for learning;

- ensure that unnecessary personal photographs, videos, messages and sensitive information are not stored on the learning device;
- support appropriate device use, digital wellbeing and responsible online behavior;
- discuss the BYOD Policy and Acceptable Use Guidelines with my child;
- monitor my child's use of the device outside school;
- inform the school if the device is lost, stolen, replaced or compromised;
- cooperate with the school in addressing misuse, safeguarding or security concerns;
- accept responsibility for the maintenance, repair, insurance and replacement of the device; and
- ensure that my child brings the device charged and ready for learning each day.

Student Commitment

As a student participating in the BYOD programme, I agree to:

- use my device responsibly, safely and primarily for learning;
- follow staff instructions about when and how the device may be used;
- comply with the BYOD Policy, Acceptable Use Guidelines and Behavior Management Policy;
- use only my own authorized accounts and protect my passwords;
- keep required security settings, applications and school configurations active;
- respect the privacy, dignity, work and personal information of others;
- use digital tools and artificial intelligence honestly and responsibly;
- avoid prohibited content, applications and activities;
- not bypass school filtering, monitoring or security controls;
- report harmful content, unsafe behavior, lost devices and security concerns promptly;
- cooperate with reasonable and authorized school investigations; and
- accept the consequences of misuse in accordance with school policy.

Parent/Guardian Acknowledgement and Consent

To participate in the BYOD programme, a parent or legal guardian must complete the electronic **BYOD Acknowledgement and Consent Form** for each student.

Please click the link below to confirm that you:

- have read and understood the BYOD Policy and Acceptable Use Guidelines;
- have discussed the requirements with your child;
- agree to support your child's compliance with the policy;
- consent to the nominated device being enrolled for access to the school's network and approved digital services; and



- confirm your child's commitment to responsible device use.

[Madar International School – BYOD Agreement and Consent Form](#)

The form must be submitted before the student's device can be enrolled in the BYOD programme.



Inspiring minds

Madar International School is accredited by **cognia**

P. O. Box 15658, Al Towayya, Al Ain, UAE,
Tel. No.: (+971 3) 7611330 / Fax No.: (+971 3) 7611511

Visit our website!



www.madarschool.ae