MAMOURA

BRITISH ACADEMY

BYOD, E-Safety and Responsible Use Policy

Policy Issued	January 2020
Policy Updated	May 2024
Next Review	May 2025
Lead Professional	Emma MacDonald
SGG Ratification	June 2024

Rationale

To ensure that there are clear guidelines that govern the use of students own devices safely and securely whilst on the school premises.

This policy includes references to the following external policies:

- ADEK Digital Policy 2024
- ADEK Behaviour for Learning Policy 2024
- MBA Compliance Policy
- MBA Staff Handbook
- MBA Inlcusion Policy

Strategic Direction

As education systems evolve to better prepare tomorrow's workforce with 21st century skills, the shift towards eLearning becomes increasingly significant, especially evident now in the current climate. The access advantage—anytime, anywhere, any device—gives BYOD a significant benefit over more traditional technology integration models.

Mamoura British Academy recognises that as technology has changed more pupils have access to Internet capable devices. This should be a resource and provide an opportunity to enable quick and easy access to the Internet to enhance learning. Devices should no longer be looked on as distractions but should be used in classrooms to aid learning.

Devices are used in lessons for a range of reasons:

- It allows for different students to complete different activities based on their level of understanding
- It enables teachers to assess students' levels in real-time during lessons to adjust their teaching based on students' understanding
- It improves collaboration and offers opportunities for students to learn together effectively
- Resources can be shared with specific students to help their understanding or challenge them
- It is more sustainable than sharing paper resources
- Students can create presentations to share their learning
- Older students can type their coursework/NEA

Across the Aldar Education group, we have implemented a digital strategy that specifies the use of Apple devices across all schools. This will allow us to roll out a range of applications and platforms and increase consistency across the group.

In addition, this will allow us to introduce a digital safety package, JAMF, to protect the students online and to support teachers in monitoring and quality assuring students' digital access.

JAMF will support learning and teaching, as well as the safety of children, in the following ways:

- **Dashboard** — Teachers and parents can keep track of managed devices, users and apps. In lessons, teachers are able to instantly see what children are accessing from their teacher's device.
- **Classroom Management** — Teachers can drag and drop apps, content and add restrictions to safeguard your children.
- **Locations** — Teachers can manage each location and its devices, users and groups

separately, pushing down profiles and apps from a single location.

- **Access** – The JAMF system will only allow users to access sites approved by the school. All other apps and programmes will be blocked, even if they are already downloaded on a students' device.

Bring Your Own Device

Year Groups and Access

All students in Year 1 to Year 13 are expected to bring their own device. For students in Year1 to Year 9, this must be an Apple iPad. For students in Year 9 and above, students can bring an Apple iPad, but a MacBook is preferable.

Device Specifications

Recommended IPAD:
1. iPad 9th Generation – 64GB
2. Logitech Combo Touch Keyboard Case
3. Stylus: Skriva

Minimum Requirements:
1. iPad 8th Generation, iPad Air 4th Generation
2. Keyboard Case
3. Stylus

Recommended MacBook:
MacBook Air 13" with M1 Chip

Minimum Requirements:
Models that are 2020+ in age

Mobile Phones

Mobile phones, including iPhones, are not permitted to be used by students anywhere on the school premises. Please refer to the Behaviour Policy for more information on sanctions around the use of phones on site.

Digital Safety Package (JAMF)

The Digital Safety Package (JAMF) is a tool that can be applied both in school and at home. There is a one-time set up cost to parents of 285dhs when installing the application on a child's device. Full details can be found on the Aldar Education E-Store which can be accessed through this link: https://aldareducation.jtrs.ae.

- In order to access internet at Mamoura British Academy, all families must sign up to the JAMF package through Aldar Education. Before adding the JAMF software, the device must be cleared of all content.
- Devices that do not have JAMF installed will not work on the school premises and cannot be brought into school.
- Only one educational device will be permitted on the Mamoura British Academy network.

Loss, theft or damage

Responsibility to keep the device secure rests with the individual owner. Mamoura British Academy or Aldar Academies are not liable for any device stolen or damages on site. If a device is stolen or damaged, it will be handled through the administration like other personal artefacts that are impacted in similar situations. Additionally, protective cases for technology are encouraged.

If a student loses their device, has it stolen or damaged whilst on the school premises or on a school sponsored trip, the school will not accept responsibility for its loss. As all students will have Apple devices, the activation of 'Find my Device' is recommended.

Responsible Use

Definition of responsible use

Responsible usage of school software and digital devices refers to the ethical, respectful, and appropriate utilisation of digital tools and resources. It encompasses the following key principles:

- Ethical Use: Using digital devices and software honestly and lawfully. This includes respecting intellectual property rights, avoiding plagiarism, and not engaging in unauthorised access or distribution of materials.
- Respectful Behaviour: Interacting with others online in a courteous and considerate manner. This involves avoiding cyberbullying, harassment, and the dissemination of harmful or inappropriate content.
- Educational Focus: Ensuring that the use of digital devices and software aligns with educational objectives and enhances learning experiences. Personal use should not interfere with academic responsibilities.
- Security and Privacy: Protecting the security of personal and school data. This includes using strong passwords, not sharing login information, and following school policies on data protection.

Permitted times and areas for use of devices

- Devices can be used only in the classroom as a learning tool under the direction of the teacher/a member of staff. A student may not take a device out of their bag unless specifically directed by a member of staff.
- Devices are not allowed outside the classroom in the corridors, playgrounds, canteen or toilets but can be used outside the classroom with interactive displays as permitted by the teacher/member of staff.
- Parents must not contact children on their device during school hours.

Note: While in ECAs or on school trips, all of the in-school expectations detailed above apply to the use of devices.

Consequences for Misuse/Disruption/Irresponsable Use

- Access to the wireless network will be removed.
- Device taken away for the period.
- Device taken away and kept with teacher until parent collection.
- In certain situations, the school is required to report any misuse to ADEK.

E-Safety

Prohibitions

The ICT resources of the school must not be used to search for, create, store, receive or transmit any materials, nor to engage in any activities, which are either illegal or prohibited by this policy. **Prohibited materials and activities are listed below**. This is a long, but non-exhaustive list. Whilst the school endeavours to educate students about all the items on this list, students (and parents) should ask for help where they are not clear about any of the issues listed.

Prohibited content and materials are those which are or may be deemed to be:

- racist, sexist or causing any form of prejudicial offence
- threatening, abusive or inciting violence
- obscene, indecent or pornographic
- age-inappropriate
- defamatory
- promoting extremist views
- promoting intolerance of the beliefs, sexuality or life choices of others
- likely to mislead or deceive others
- likely to cause unnecessary stress or anxiety to others
- anything deemed to be culturally inappropriate

Prohibited activities include:

- bullying (also known in this context as cyber-bullying – see our Anti Bullying Policy)
- Harassment – unwanted attention, pestering or persecution (including insults and 'jokes')
- arranging to meet in person with someone first met online (without first checking with parents or teachers)
- writing or posting content on the internet, social media, or school network anything which may cause harm or offence to other children, parents, staff or to the school
- sexting
- 'trolling' – mischievously or maliciously upsetting or offending people on the internet or social media by posting inflammatory remarks
- pretending to be someone else, or theft of someone's identity
- gambling
- promotional, advertising or other commercial activities (unless authorised by staff)
- hacking (deliberate unauthorised access to websites, devices, networks, systems or databases)
- taking photographs and making audio or video recordings of other people, and distributing such images or recordings, without first obtaining their permission
- unauthorised uploading, such as software licensed to the school, or data owned or protected by the school or by others
- use of peer-to-peer (P2P) sites or networks unless explicitly authorized by the ICT Leader
- activities that might:
  - waste staff effort or network resources
  - corrupt, delete, or destroy other users' data

- violate the privacy or other rights of other users
- disrupt the work of, or deny service to, other users
- anything deemed to be culturally inappropriate

- activities that might affect the proper functioning of ICT resources such as:
  - disabling or overloading any computer system or network,
  - attempting to disable, defeat or circumvent any system intended to protect privacy, security, or intellectual property rights (e.g. copyright)
  - installing or connect any devices, software applications (including games) without authorisation
  - altering system settings, desktop wallpapers, icons etc. without authorisation
  - introduce viruses, worms, Trojan horses, trapdoors or similar programmes
  - interfering with power supply or data cabling

Responsibilities of the School

As a school, we are committed to the education of students and families on the ways in which we can safeguard children against the risks they may encounter online.

- Education Programmes: Mamoura British Academy will provide educational programmes linked to e-safety for all students in the school. This will incorporate educating them to:
  - Understand what constitutes inappropriate or illegal content, or content that may be detrimental to their wellbeing.
  - Be aware of unsafe online interactions such as fake profiles.
  - Be aware of what constitutes cyberbullying and the implications to them if they are involved in cyberbullying.
  - Identify and report online behaviour that can lead to self-harm for others (i.e cyberbullying).
  - Identify scams and finance related risks such as gambling and phishing
  - Identify and acknowledge risky or excessive online behaviour such as digital addiction or gambling in line with the ADEK Student Mental Health Policy and the ADEK Student Behaviour Policy.
- Digital Technologies for Advancement of Learning:
  - Staff at Mamoura British Academy will ensure that the use of digital devices is always used for the development of learning.
  - The resources, applications and Ed-Tech sites provided by staff will be checked before being accessed by students. This is inline with our Compliance Policy.

Responsibilities of Students

All students are encouraged to use ICT resources to support their programmes of learning. Students have no right to use ICT resources for other purposes (e.g. personal recreational, administrative, or commercial) which are not connected to their programme of learning.

Students are expected to:

- ask questions and share any concerns or confusion they have about how to interact with ICT.
- demonstrate a responsible approach to ICT usage, show consideration for all other users, and treat ICT resources with care and respect.

- be clear, polite, respectful and responsible in all electronic communications and use of social media, remembering that they must not write, nor post on-line, anything which could embarrass themselves, other children, staff, parents or the school if it later became more widely seen than was originally intended.
- only access files on the computer or internet sites which are relevant to classroom curriculum.
- TEAMS will often be used as a means of teaching, especially for home learning and remote learning purposes. The chat function for this programme is disabled for all students.
- understand that printing from their personal device may not be possible at school.
- obtain permission from a staff member before connecting any personal electronic device with the ICT resources of the school; removable storage (memory sticks, external hard drives, CDs/DVDs) must be virus-checked before being connected to the school ICT resources.
- observe all the conditions of usage laid out in this policy, **avoid the prohibited content and activities as listed**, and follow the direction of staff members supervising any area where networked resources can be accessed.
- report immediately to a staff member wherever they encounter breaches in the controls and security of the network, or where they observe any abuse of ICT resources.
- in using the network and Internet, users should not reveal personal information such as a home address or telephone number.
- students may not record, transmit or post photographic images or video of a person, or persons without their permission.
- avoid engaging in cyberbullying, harassment, or disrespectful conduct toward others--staff or students.
- avoid using language online that would be unacceptable in the classroom.

MBA IT has the right to collect and inspect any device that is suspected of causing problems or is the source of an attack or virus infection.

Any child who knowingly abuses the privileges of ICT resources will face disciplinary procedures in line with the school and ADEK Behaviour for Learning Policy.

Consequences for Misuse/Disruption/Irresponsible Use

- Access to the wireless network will be removed.
- Device taken away for the period.
- Device taken away and kept with teacher until parent collection.
- In certain situations, the school is required to report any misuse to ADEK and/or the Abu Dhabi Police.

Responsibilities of Staff and Parents

The prohibitions listed will have little significance and effect in practice without an ongoing commitment by staff and parents to:

- promote understanding amongst students of why things are prohibited.
- stay vigilant to the actual behaviour of students in their interaction with ICT.

- establish an environment where students are encouraged to talk and ask questions about their interaction with ICT, and where they can feel safe sharing their concerns.
- talk to each other (parents and staff) to share information and concerns.
- for staff to follow the guidelines as outlined in the Staff Handbook.
- for staff to educate students on the importance of e-safety within the school curriculum.

Controls, privacy and reporting of breaches

Log-on details (account names and passwords) for access to ICT resources must be kept secret and must not be written down or shared. All users must remember to log-off when they are not in close physical proximity to the machine or device to which they are logged-on. Computers and other user-controlled ICT resources should be either switched off or put on 'stand-by' after use, and especially at the end of the day. If passwords are shared students are expected to change them immediately.

In accordance with statutory guidance, and with the aim of mitigating the risk of harmful behaviour and access to harmful materials, the school ICT resources are subject to various preventative and detective controls such as anti-virus protection, internet- and email-filtering, and usage-monitoring. Consequently, students should not expect their usage of school ICT resource (including email and internet browsing), nor any of the material they store using school ICT resources, to be private or confidential. The school has the right to search and delete any material where it has grounds to suspect that such material may be harmful to the welfare of students.

Staff must remain alert to actual and potential breaches of security and of prohibited content and activities. Students are encouraged to look after each other, and to tell staff if they become aware of prohibited content or activities, or weaknesses in network security or internet filtering. Staff must report actual or potential breaches or weaknesses to the ICT technicians and the Heads of Primary & Secondary, in addition to any other reporting processes as required by other policies (Safeguarding, Anti-Bullying, E-Safety), for example to the Designated Safeguarding lead (DSL).

Responsibility for the practical implementation of this policy

a) Security and effectiveness of the ICT resources and infrastructure

The development and maintenance of ICT services and controls, including data protection, network security and internet filters are the responsibility of the **Aldar Group Director of ICT**, and are administered through a team of **On-Site Engineers** assigned to each group location. This technical team has a key role in maintaining a safe technical infrastructure and in keeping abreast with the rapid succession of relevant developments in technology and new media.

In order to ensure the effective operation of ICT services and controls it is essential that a member of school staff is nominated as ICT technician and is assigned responsibility for monitoring the effective delivery of such services on behalf of all school users, and for reporting weaknesses and opportunities for improvement where necessary.

b) Broader welfare issues of E-safety

The **Designated Safeguarding Lead (DSL**) has been trained, and updates their training regularly, in the safety issues relating to the misuse of ICT resources.

All staff have an ongoing responsibility to reinforce this policy with students and (where practical) to monitor that their usage of ICT is in compliance with the policy. Serious or persistent breaches must be reported to the Lower School or Middle and Senior School Principals and (if safeguarding issues are suspected) to the DSL.

All parents are asked to give consent for their child's image to be used within the school and for social media and marketing purposes. A record of those students who do not have media permission is kept with the PRE.

Copyrighted Materials and Digital Tools (in accordance with Federal Decree #38)

Use of educational materials both digitally and paper-based must be in line with copyright regulations of the publisher. This is not limited to, but for example the use of White Rose Maths resources, in which Mamoura British Academy employees with access have agreed to:

- not use the Resources or Goods in any way which is defamatory, indecent or otherwise unlawful or which infringes the statutory or common law rights of any third party;
- not redistribute the Resources or use any part of the Resources in any products or services it offers commercially;
- only use the Resources and Goods for the Permitted Uses, and not use the Resources or Goods outside of the User's usual teaching or tutoring premises;
- procure that all descriptive literature relating to the Resources be marked with a notice in the following terms: © Copyright [add in who it is copyright to];
- not remove any mark, notice or wording on the Resources which acknowledges ownership of the Resources or the fact that the Resources are subject to copyright, the rights to which belong to the provider (for example White Rose Maths);
- on termination of this Licence either destroy or return all copies of the Resources and/or the User's materials which are based on the Resources;
- not do or omit to do anything to diminish the rights of the producer in the Rights, the Goods or the Resources, nor assist any other person to do so, either directly or indirectly and not alter or modify the Resources or Goods;
- on reasonable notice, provide the company producing the resources with access to all documents, records and materials relating to your use of the Resources, for the purpose of the producer of the resources checking your compliance with this License.

Staff are requested to review the copyright and user obligations of all purchased resources.

Academic Honesty

Scope

Academic honesty encompasses all forms of academic work, including but not limited to assignments, exams, projects, and research.

Principles of Academic Honesty

- Integrity: Students and staff must act with honesty and integrity in all academic

activities.
- Responsibility: Individuals are responsible for their own work and must ensure it is free from dishonesty and misrepresentation.
- Respect: Respect the work and intellectual property of others by properly acknowledging and citing sources.

Prohibited Conduct
- Plagiarism: Presenting someone else's work, ideas, or data as one's own without proper attribution.
- Cheating: Using unauthorized materials, information, or assistance in any academic exercise.
- Fabrication: Falsifying or inventing any information or data in academic work.
- Facilitating Academic Dishonesty: Helping or attempting to help another student commit an act of academic dishonesty.

Use of AI in Academic Work
- Permissible Use:
  - AI tools may be used for research, data analysis, and other purposes as explicitly allowed by instructors.
  - Students must clearly acknowledge the use of AI tools and specify how these tools were used in their work.
- Prohibited Use:
  - Using AI to generate text, images, code, or other content that is submitted as one's own work without proper attribution.
  - Submitting AI-generated content as original work without disclosure and instructor approval.
- Guidelines for Ethical AI Use:
  - Always disclose the use of AI tools in your work.
  - Attribute any AI-generated content appropriately, just as you would with other sources.
  - Use AI to complement, not replace, your own learning and creativity.

Responsibilities
- Students:
  - Adhere to this policy in all academic activities.
  - Seek clarification from instructors if unsure about the use of AI or other resources.
  - Report any observed instances of academic dishonesty.
- Faculty and Staff:
  - Communicate clear guidelines regarding academic honesty and the use of AI tools in their courses.
  - Model academic integrity in their own work.
  - Report and address violations of this policy according to established procedures.

Procedures for Addressing Violations
- Reporting:
  - Suspected violations should be reported to the relevant faculty member or academic integrity office.
  - Reports can be made by students, faculty, or staff.
- Investigation:
  - The academic integrity office will investigate reported violations.
  - Students will have an opportunity to explain their perspective during the investigation.

- Consequences:
    - Consequences for violations may include a failing grade on the assignment, a failing grade in the course, academic probation, or expulsion, depending on the severity of the violation.
    - Repeat offenses will result in more severe penalties.

Education and Prevention

- Training:
    - The school will provide regular training for students, faculty, and staff on academic integrity and the ethical use of AI.
    - Resources and workshops will be available to help students understand how to properly use and cite AI tools.
- Resources:
    - The school will maintain resources such as guides, tutorials, and consultation services to assist students in adhering to academic honesty principles.

Assistive Technology

Assistive technology (AT) is essential for supporting the diverse learning needs of students, including those with disabilities and learning differences. Mamoura British Academy is committed to fostering an inclusive environment where all students have equitable access to educational opportunities. Further information about the use of Assistive Technology can be found in the Mamoura British Academy Inclusion Policy.

Definition of Assistive Technology

Assistive technology refers to any device, software, or equipment that helps students with disabilities or learning differences perform tasks that might otherwise be difficult or impossible. This includes, but is not limited to:

- Speech-to-text and text-to-speech software
- Hearing aids and FM systems
- Screen readers and magnification software
- Communication devices
- Adaptive keyboards and mice
- Educational apps designed for special education

Principles and Objectives

- Inclusion: Ensure that all students have access to the tools they need to participate fully in their education.
- Equity: Provide equal opportunities for students to succeed, regardless of their abilities.
- Support: Offer adequate support and training for students, teachers, and parents on the use of assistive technology.
- Confidentiality: Respect the privacy and dignity of students using assistive technology.

Responsibilities

- Principal/Headteachers:
    - Ensure that the school infrastructure supports the use of assistive technology.
    - Allocate funding and resources for the procurement and maintenance of assistive technology.
    - Provide training for staff on the effective use and integration of assistive technology in the classroom.
- Teachers:
    - Incorporate assistive technology into lesson plans and classroom activities.
    - Participate in training sessions on the use of assistive technology.

    - Monitor and support students' use of assistive technology to ensure it is effective.
- Students:
    - Use assistive technology responsibly and for its intended purpose.
    - Report any issues or malfunctions to their teacher or the IT department.
    - Participate in training sessions to maximize the benefits of the technology.
- Parents and Guardians:
    - Support their child's use of assistive technology at home.
    - Attend informational sessions and training offered by the school.
    - Communicate with teachers and school staff regarding their child's needs and progress.

Implementation and Use

- Assessment and Planning:
    - Conduct assessments to identify students who may benefit from assistive technology.
    - Develop Individualized Education Plans (IEPs) or equivalent documents that outline the specific assistive technology needs and strategies for each student.
- Training and Support:
    - Provide ongoing training for teachers, students, and parents on the effective use of assistive technology.
    - Offer technical support to troubleshoot and maintain assistive technology devices and software.
- Integration in the Classroom:
    - Integrate assistive technology seamlessly into daily classroom activities and curricula.
    - Ensure that assistive technology is used to enhance learning outcomes and not as a substitute for instruction.

Evaluation and Monitoring

- Regular Review:
    - Conduct regular reviews of students' progress to assess the effectiveness of assistive technology.
    - Update IEPs or equivalent documents as necessary based on the students' evolving needs.
- Feedback Mechanism:
    - Establish a feedback mechanism for students, parents, and teachers to share their experiences and suggestions regarding assistive technology.
    - Use feedback to make continuous improvements to the assistive technology program.

Privacy and Security

- Data Protection:
    - Ensure that all data related to students' use of assistive technology is stored securely and handled in compliance with data protection laws and school policies.
    - Maintain confidentiality of student information at all times.
- Ethical Use:
    - Promote the ethical use of assistive technology, ensuring it is used solely for educational purposes and in a manner that respects the dignity of all students.

Parental Expectations

In an increasingly digital world, parental engagement is an important aspect of monitoring internet use and children's safety. Parents are expected to monitor students' usage of digital devices outside of school premises and school hours to ensure safe and appropriate digital behaviour.

Agreements

In order to ensure that all parties agree to the terms and conditions of the BYOD policy it is essential that all parents and students sign the agreements advocated by Adlar Education. By signing these agreements it confirms that all parties are aligned to the acceptable use of devices within the school premises.