

BRING YOUR OWN DEVICE (BYOD) POLICY FOR STUDENTS

ABOUT THIS POLICY

Al-Ameen College recognises that personal electronic devices, used for learning purposes, can have significant benefits for both students and teachers, including increased learning flexibility, in permitting such use. We understand that such technology offers valuable benefits to staff and students from a teaching and learning perspective. Our school embraces this technology but requires that it is used in an acceptable and responsible way.

However, the use of personal devices for learning by students, has with it, increased risk in terms of the security of school IT resources, communications systems and the protection of confidential information.

This policy is intended to address the use by students and staff members of non-school owned electronic devices (referred to as the 'device' in this policy) to access the internet via the school's internet connection and/or to access or store school information.

Anyone covered by this policy may use the device for learning and teaching purposes, provided that students sign the declaration at the end of this policy and adhere to its terms.

This policy sets out the conditions through which students and teachers may bring their own device into school to use for educational purposes.

SCOPE AND PURPOSE

This policy applies to both students and staff who use a personal electronic device including any accompanying software or hardware for learning purposes. The policy applies to all devices used to access our IT resources and communications systems (collectively referred to as 'systems' in this policy). It applies to the use of the device both during and outside school hours whilst on the school site.

When you access school systems using a device, the school is exposed to a number of risks, including the threat of malware (such as viruses, worms, spyware, Trojans or other threats that could be introduced into our systems via a device). This could result in damage to school systems.

The purpose of this policy is to protect school systems while enabling you to access our systems using a device. This policy sets out the circumstances in which we may monitor your use of school systems, access your device and retrieve, remove or destroy data on it, and the action which we will take in respect of breaches of this policy.

Breach of this policy may lead to the school revoking your access to school systems, whether through a device or otherwise. It may also result in sanctions up to and including exclusion. You are required to co-operate with any investigation into suspected breach, which may involve providing us with access to the device and any relevant passwords and login details.

Some devices may not have the capability to connect to school systems. The school is not under any obligation to modify its systems or otherwise assist students in connecting to those systems.

In addition, Al-Ameen College is committed to meeting its legal and duty of care obligations while providing a flexible environment to allow students and staff to bring their own devices to school. As stated, the use of an own device also introduces new risks in protecting the integrity, confidentiality and privacy of all concerned.

Whilst every care is taken to ensure that the school puts in place all security and privacy measures, it should be noted that we do not have control on the security mechanisms implemented outside the school premises. Therefore, if the device was compromised, lost or stolen there would be a risk that any information stored on it could be accessed and exploited by unauthorised individuals.

PERSONNEL RESPONSIBLE

The Senior Management Team has overall responsibility for the effective operation of this policy but has delegated day-to-day responsibility for its operation to the IT Technician. The Senior Management Team shall be responsible for reviewing this policy to ensure that it meets legal requirements and reflects best practice.

All staff and students at Al-Ameen College are responsible for the success of this policy. Any misuse (or suspected misuse) of a device or breach of this policy should be reported to a member of Senior Management immediately.

TERMS

Parent/Students Agreement

Parents and students must agree and sign to the contents of this BYOD policy to show acceptance of the terms and conditions of the use of personal electronic devices in school before students are permitted to use their own device.

Personal Electronic Devices (referred to as the 'device' in this policy).

Such devices include laptops, notebooks, and two-in-one devices. iPads are not allowed. Mobile devices such as smartphones or tablets are not allowed.

Lost, Stolen or Damaged

Students and teachers who bring devices into school do so entirely at their own risk, just like any other personal item. Al-Ameen College will not accept any responsibility for devices that are miss-placed, lost, stolen or damaged.

Many devices have a location finder app and it is recommended that this feature is enabled to aid tracking, wherever possible. It is also recommended that such devices are fully insured on individual family's home contents insurance to cover loss and damage outside of the home, or through a device/gadget specific insurance policy. In the event of a lost or stolen device, you should report the incident to the Main School Office.

Security and Care

Students and teachers are responsible for the proper care and use of their own device, as well as the adequate security of such whilst at school. Students always need to keep their device

with them (when required) or properly secure it in their lockers when not in use. It is recommended that students do not share or lend their device to other students.

Educational Use

Students that have signed and submitted the “Bring Your Own Device Declaration & Agreement” below will appear in the class register as having done so and their devices will only be used for educational purposes to support learning whilst in school. It will be at the teacher's discretion as to when these devices may be used by a student within school. Students will respect a teacher's decision and turn off their device when requested to do so.

Outside of their classroom hours, students should refrain from using devices at school. In the event that they require usage during these times, they must seek permission from the librarian and use the devices within the library premises.

Audio, Photographs and Video

Students should not use their device to record audio or take photographs or video of other students or members of staff without their permission and should not transmit or upload onto social media.

Hotspot

Under no circumstances are students allowed to Hotspot via any other device.

Internet Usage Policy

Devices will only access the internet through the Al-Ameen College network. Students will adhere to the school's ICT Acceptable Usage and Guidelines Policy whilst on the school site. In addition, students and staff will not access any inappropriate material that may or may not already be downloaded onto their device. Members of staff have the right to access a student's own device if there is reason to believe a student is in violation of this policy or the above-mentioned policy.

Appropriate Use

You should never access or use school systems through a device in a way that breaches this policy or the school's ICT Acceptable Usage and Guidelines Policy. If you breach this policy, you may be subject to sanctions up to and including exclusion.

Sanctions for Misuse Including Accessing Non-Permitted Sites

In the event of misuse, a student may be refused permission to use personal devices at school and access to the wireless network will be removed. Misuse of internet capable devices will be regarded as a serious offence. The student will also be referred to the Assistant Principal Wellbeing.

Failure to comply with this policy may result in the revocation of access to the school systems. It may also result in disciplinary action being taken against the student, which if serious, may lead to dismissal. Students are required to co-operate with any investigation into a suspected breach, which may include providing us with access to the device.

STUDENTS BREACHING BYOD POLICY

If a student breaches the BYOD Policy or if a member of staff feels that they are likely to have breached this policy, then the student's device will be confiscated and held in the school office.

The student's parent will be contacted, and they will need to come into school to collect the device. Subsequent breaches of this policy by the same student will result with that student no longer permitted to bring in their own device.

REQUIREMENTS & RECOMMENDATIONS FOR DEVICES

To ensure the correct device is purchased we have outlined the following minimum requirements, recommendations, and security guidelines.

- Processor: Intel Core i3 10th Generation or AMD Ryzen 3 3rd Generation – 2020
- Memory: Minimum 8GB.
- Hard Drive: 256GB SSD.
- Antivirus: One of the recommended products:
 - Norton 360 Deluxe.
 - McAfee Internet Security.
 - ESET Smart Security Premium.
 - Kaspersky Total Security.
- Battery duration: at least 4-6 hours.

Requirements for an APPLE Device

- Mac OS 10.14 or later
- At least a 13" display
- At least Intel i3
- At least 8GB Ram, at least 256GB SSD and Wi-Fi capability

MICROSOFT OFFICE

Al-Ameen College will be providing students with free Microsoft Office 365. This software is required for students to perform their daily tasks such as create, edit and store files. Students should bring their laptops with Microsoft Office installed and activated.

We strongly recommend students not to buy Microsoft Office from manufacturers or retail stores.

EXTENDED WARRANTIES

If affordable, we recommend purchasing an extended warranty that covers three to four years. Where possible, purchase additional protection that covers drops and liquid damage to the device.

ACCESS TO THE SCHOOL'S INTERNET CONNECTION

Connectivity of all devices is centrally managed by the Al-Ameen College IT Technician once a device is approved by the school.

Whilst the device belongs to the student, the school provides a wireless network that students and staff may use to connect their devices to the Internet. Access to the wireless network is at the discretion of the school, and the school may withdraw access from anyone it considers is using the network inappropriately.

Whilst every precaution is taken to ensure that the school's wireless network is secure, students and staff use it at their own risk.

The school is not to be held responsible for the content of any apps, updates, or other software that may be downloaded onto the user's own device whilst using the school's wireless network. This activity is taken at the owner's own risk and is discouraged by the school. The school will have no liability whatsoever for any loss of data or damage to the owner's device resulting from use of the school's wireless network.

All devices should only link up with the internet via the School wireless network. This access is logged and filtered appropriately. The primary purpose of the use of personal devices at school is educational and to facilitate communications between staff and students. Students must ensure that the device, while connected to the school network, is not used for any purpose that would be at odds with this policy.

The school reserves the right to refuse or remove permission for your device to connect with school systems. In such cases, Al-Ameen College will refuse or revoke such permission (and may take all steps reasonably necessary to do so) where in our reasonable opinion a device is being or could be used in a way that puts, or could put, the school, our students, our staff, our systems, or sensitive school data at risk or that may otherwise breach this policy.

To access school systems, it may be necessary for our IT Support to install software applications on your device. If you remove any such software, your access to our systems will be disabled.

In-Class use

In order to participate in the class activities, students are required to install a monitoring system that aims to assist the teacher with delivering the class content properly, avoiding any distractions which can interfere with the class flow or students' performance.

This software does not allow teacher to have access to students' personal files, however it does require student approval of the 'share screen' feature for each class.

Teachers are required to ensure that all students are connected to the monitoring system at the beginning of each class.

ACCESS TO THE SCHOOL IT SERVICES

Students and staff are permitted to connect to or access the following school IT services from their devices:

- the school email system (where appropriate encryption technologies have been deployed).
- the school virtual learning environment (Google Classroom, Office 365 and 'School Drives').
- official school apps such as NAPLAN, OLNA, Maths Space, Browsers, etc
- SEQTA Teach and Learn.

Students may use the systems listed above to view school information via their devices, and store necessary information on their devices, or on their OneDrive cloud storage. Students must only use their devices for work purposes.

School information accessed through these services is confidential, and students must take all reasonable measures to adhere to this policy.

Users must follow the procedures for connecting to the school systems as set out by the IT Services Department.

We have an ICT Department that provides support for students, staff and parents. The contact is itsupport@alameencollege.wa.edu.au. The received e-mails will raise a new ticket in our system, which will be classified and attended to according to its priority level.

CHARGING THE DEVICE IN SCHOOL

The device's charger must be certified and able to be plugged into an electrical socket on school site. The school will look at providing docking stations for students to use.

MONITORING USE

The school reserves the right to monitor, intercept, review and erase, without further notice, content on the device that is deemed to be in breach of this policy.

The school uses technology that detects and monitors the use of devices which are connected to or logged on to our wireless network or IT systems. By using your device on the school's IT network, students agree to such detection and monitoring. The school's use of such technology is for the purpose of ensuring the security of its IT systems and for tracking school information.

The information that the school may monitor includes (but is not limited to) the addresses of websites visited, the timing and duration of visits to websites, information entered into online forms (including passwords), information uploaded to or downloaded from websites and school IT systems, the content of emails sent via the network, and peer-to-peer traffic transmitted via the network.

Students who receive any inappropriate content through school IT services or the school internet connection should report this to the school's IT Technician as soon as possible.

Monitoring, intercepting, reviewing or erasing of content will only be carried out to:

- prevent misuse of the device.
- ensure compliance with our rules, standards of conduct and policies in force from time to time (including this policy).

By signing the declaration at the end of this policy, you confirm your agreement (without further notice or permission) to such monitoring. You also agree that you use the device at your own risk and that the school will not be responsible for any losses, damages or liability arising out of its use, including any loss, corruption or misuse of any content or loss of access to or misuse of any device, its software or its functionality.

SECURITY REQUIREMENTS

You must comply with our ICT Acceptable Usage and Guidelines Policy which is available on the main website when using your device to connect to school system. The school reserves the right, without further notice or permission, to inspect your device and access data and applications on it, and remotely review, copy, disclose or wipe, enabling us to:

- inspect the device for use of unauthorised applications or software.
- investigate or resolve any security incident or unauthorised use of school systems.
- ensure compliance with our rules, standards of conduct and policies in force from time to time (including this policy).

You must co-operate with the school to enable such inspection, access and review, including providing any passwords or pin numbers necessary to access the device or relevant applications. A failure to co-operate with the school in this way may result in sanctions, up to and including expulsion.

If the school discovers or reasonably suspects that there has been a breach of this policy, including any of the security requirements listed above, your access to school systems will be immediately removed.

By signing the declaration at the end of this policy, you consent to the school, without further notice or permission, inspecting a device and applications used on it, and remotely reviewing, copying, disclosing, wiping or otherwise using data on or from a device that is in breach of this policy.

TECHNICAL SUPPORT

We do not provide technical support for devices. If you bring your device to school, you are responsible for any repairs, maintenance or replacement costs and services.

COSTS AND REIMBURSEMENTS

By signing the declaration at the end of this policy you acknowledge that you/your parents alone are responsible for all costs associated with the device and that you understand that your usage of the device in school may increase any data usage charges.

KEY RELEVANT DOCUMENTS

ICT Acceptable Usage and Guidelines Policy
Al-Ameen (BYOD) Rationale Strategy 2023-2024

FREQUENTLY ASKED QUESTIONS (FAQS)

How often will a student use a device in lessons during the course of a school day?

We are looking at increasing the use of technology in lessons which will be done through the sharing of resources within our Office 365 platforms and unlocking the study potential through these and the internet. We cannot be sure exactly how often devices will be used each school day, but staff will purposely plan for the use of technology when it is appropriate for the lesson. Learning in school will also be connected to learning at home through the platforms.

Will it be possible to charge the device during the school day?

The device may be charged but the opportunity to do so may be limited by the availability of a socket. Therefore, please ensure that the device is charged overnight and ready for use in school, using its own battery power.

Does the school network have the capacity for large numbers of students to use devices at the same time?

Recognising the potential in developing learning using technology, we have stepped up our network. This greatly increases the capacity and security of the network, as well as increasing the speed of our internet service, allowing for the increase in devices being used on the school site.

Which sites are not permitted and blocked?

It is illegal to access the following sites which, amongst others, have been blocked: online games, pornography, deep web, gambling, social media sites such as FB, Instagram, YouTube, Twitter, etc.

REVISION HISTORY

NAME	ACTION	DATE
NM	Initial Document	23/11/2022
JC/KH	Update	31/01/2023
RA/FP	Update	13/06/2023
FP/PR	Review	20/01/25

BRING YOUR OWN DEVICE DECLARATION & AGREEMENT

Parents/Guardians and Students - Please sign the BYOD agreement to agree to the contents of this policy.

Students will be unable to use their own device in school unless both parties (parent and student) agree to the contents of this policy.

STUDENT NAME		CLASS	
PERSONAL ELECTRONIC DEVICE DETAILS			

TYPE	
MAKE	
MODEL	
SERIAL NUMBER	

I wish to use the above detailed personal electronic device for learning purposes at Al-Ameen College and explicitly confirm my understanding and agreement to the following:

- I have read, understood, and agree to all the terms contained in the Bring Your Own Device (BYOD) Policy.
- I understand that the terms of this policy will apply to me at all times, during or outside school hours, when I am on the school site.
- I acknowledge and agree that authorised personnel of Al-Ameen College shall have the rights set out in this policy, including but not limited to the right to access, monitor, review, record and wipe (as the case may be) data contained on my personal device (which I acknowledge may result in inadvertent access to or destruction of my personal data).
- I understand and agree that Al-Ameen College in its discretion may amend or remove this policy at any time and that I will be bound by the terms of the policy, as amended.

As an Al-Ameen College student, I understand and agree to the conditions set out in the BYOD Policy. I understand that if I breach this policy, my device may be removed and held in the school office to be collected by my Parent/Guardian. I also understand that I may lose the privilege of bringing my own device into school and possibly face sanctions.

SIGNED (STUDENT)

DATE

As an Al-Ameen College Parent/Guardian, I understand that my child will be responsible for adhering to this policy. I have read and discussed this policy with my child, and they understand the trust and responsibility required in having their own device in school.

SIGNED (PARENT/GUARDIAN)

DATE