# Australian Islamic College of Sydney

## AICS BYOD Policy

Australian Islamic College of Sydney policies have a commitment to Australian Islamic ethos and values, and should be read in conjunction with other policies and procedures and with relevant legislation.

**POLICY REVIEW**

The policy will be reviewed not less frequently than once every two years.

| **POLICY DATES** | | | |
|---|---|---|---|
| Implemented | March 2023 | Reviewed | March 2023 |
| **Next Review Due** | | March 2025 | |
| **POLICY OWNER** | | **POLICY APPROVER** | |
| Mohammed Riaaz Ali<br>PRINCIPAL | | AICS Board | |

**Preface**

At Australian Islamic College of Sydney (AICS) ICT, we strive to facilitate the Teaching and Learning activities such that staff and students get the best of facilities that modern technology has to offer and enrich their learning experience and broaden their outlook.

The Bring your Own Device (BYOD) service provides Wi-Fi access to the Internet by allowing the staff or student's own personal devices to join the AICS network in a secure manner. BYOD does not provide access to any AICS internal resources such as printers, servers, etc.

AICS ICT has taken as much precautions as possible to restrict access to controversial materials on the Internet. Although AICS ICT filters and checks contents that are not consistent with Islamic Ethos and education objectives, it is impossible to filter all controversial or inappropriate materials available on the Internet. AICS ICT believes that the valuable information and interaction available on the Internet far outweighs the risk of misuse or having to face unintended consequences. All users are strongly recommended to exercise due diligence in what they access via the BYOD services and do not access unnecessary contents.

All staff, students and other users are exhorted to read the terms and conditions of AICS BYOD Policy, understand their significance, agree to it and abide by it.

**Applicability and Coverage**

This policy compliments all current AICS policies and covers the Bring Your Own Device (BYOD) service for the user community. This document does not substitute or overwrite any other policies of AICS.

**User Community**

The target user community for this policy are all students, staff of AICS, and those who use the AICS systems and facilities for short or temporary periods, such as visitors, apprentices, contractors or casual teaching and non-teaching staff.

**Service Specification**

Bring Your Own Device (BYOD) service at AICS refers to students and staff bringing their personally owned device to AICS campus, configuring and connecting to the AICS network to access the Wi-Fi (Internet) services for the purpose of Teaching & Learning.

AICS BYOD services are available to staff and High School students only during school hours and on campus only. Wi-Fi Connection (connection to College's Wi-Fi network for internet) will be provided by ICT during these times on campus. The ICT team will not provide any other technical support for any BYOD devices.

All users are allowed only one personal device per person.

**BYOD Device Specification**

All devices that intend to use AICS BYOD service must meet the requirements listed in Device Specification section in order to be able to connect to the college's Wi- Fi.

AICS cannot support devices that do not meet these requirements.

Mobile phones are not considered a BYOD device.

**Conditions of Use**

1. **Expectation of Privacy**

AICS respects the privacy of each and every person as promulgated by the Privacy Laws in Australia.

However, for the security and well-being of all users, AICS ICT routinely monitors usage of Intranet/Internet and may review any communications on its systems. AICS ICT is able to override all passwords. Users do not have a privacy right in the contents of their computer system, including messages sent, received, or stored on the email systems or in their use of the Internet. Passwords to these systems exist for the benefit of AICS. Users should not assume that the ability to choose a password for a system in any way limits the ability or right of AICS to monitor all activity on BYOD services and on the AICS network (as long as they are using AICS Wi-Fi internet)

2. **Security**

Security is a main consideration in BYOD service and is stringently observed. No user may attempt to access another user's files stored internally or any externally subscribed AICS storage or applications services. The following guidelines will help maintain Information security and Network security:

a) If users feel they have identified a security problem on the Intranet or any externally subscribed AICS storage or applications services, they must notify the ICT Department immediately.
b) No user should allow anyone else to use his/her account and do not use another individual's account.
c) Attempts to access or acquire higher level of access rights or administrator access on any AICS device or AICS's external services will result in immediate suspension of the user's account and privileges. Disciplinary action will follow.
d) Any user identified as a security risk or having a history of problems with other users or computer systems may be denied access to the AICS ICT facilities held internally as well as AICS's externally acquired services.

3. Proper Use of BYOD Bandwidth

a) Students and staff must evaluate the reliability of the source of information, as well as the correctness of contents, to ascertain its usefulness and appropriateness based on the Islamic Ethos and overall rules of AICS.
b) Access to AICS's Wi-Fi via BYOD Service will allow students and staff to communicate directly with people around the world via a variety of private messaging and audio-visual applications such as Microsoft Teams, Zoom, Skype, etc. Also, there are many free services and software technologies that will allow for exchange of files between computers over the Internet, such as email, OneDrive, Drop Box, Google Drive, etc.

Not all of these might be applicable or appropriate for AICS educational environment. Students and staff must use only applicable, appropriate and relevant applications.

c) Whilst reasonable use of AICS BYOD bandwidth or capacity to download or upload applications and data by staff and students is acceptable, excessive and frequent use of BYOD Wi-Fi for downloading and uploading is not allowed. Such actions will have a negative effect on AICS's network capacity, and can result in the substantial degradation of network performance. Such actions should be based on necessity only.
d) Downloads and uploads will cost additional ICT maintenance time and effort. It also increases security risks of spyware, malware and virus infestation. Hence it should be avoided when possible.

**4. Inappropriate Use of BYOD services**

The followings constitute inappropriate use of the AICS BYOD Wi-Fi services.

i. Students should not use BYOD to access any website, portal, streaming services, commercial services or sites that contain information that is inappropriate for or irrelevant to student's educational activities.
ii. Students may not visit or access sites or services that teachers, staff or administration deem inappropriate for the instructional program.
iii. Students should not access, upload, download, transmit, copy, display or distribute contents that is offensive to Islam and its teachings. Such contents include insulting or mocking religious sensitivities of any religion, obscene, abusive, sexually explicit language and threats.
iv. Students should not access, upload, download, transmit, copy, display, send links of any content that is considered racist, religious vilification, harassment, illegal or inflammatory.
v. Students should not access, upload, download, transmit, copy, display, send links of any content that provides direction in the construction of explosives or similar devices or instruction or practices that could injure the students themselves or others.
vi. Students should not access, upload, download, transmit, copy, display, send links of any content to fellow students or anyone that provides inappropriate contacts that can lead to contact with strangers who could potentially harm the health, safety or mental well-being of anyone.
vii. Students should not access, upload, download, transmit, copy, display, send links of any content that are bullying or threatening to anyone or anywhere, internal or external to AICS.
viii. Students should not watch, upload, download, display, send links of audio-visual streaming material not related to student's education.
ix. Students should not install a VPN on their personal devices. If any student's BYOD device has a VPN installed, the ICT team will not provide any Wi-Fi connection to the school network. If any student is found using a VPN in school, after connecting to the school Wi-Fi network, his/ her access will be disabled and disciplinary action will be taken.

If a student is uncertain as to whether or not any material might be considered inappropriate, the student should consult with their teacher or the ICT team for clarification.

### 5. User Obligations

All users who use the AICS BYOD service are bound by this policy and agree to abide by it.

**Device Specification Section**

All devices that are intended for using the AICS BYOD service must meet the following minimum requirements.

**Hardware**

| | |
|---|---|
| **Device Type** | Any Microsoft Windows or Apple (*macOS)* based laptop or tablet with keyboard or with detachable keyboard.<br>All other platforms are not supported. |
| **Memory (RAM)** | 8 Gb (Minimum)- 16 Gb (Gb stands for Giga bytes) |
| **Harddisk** | 128 Gb (Minimum) -256Gb (Gb stands for Giga bytes) |
| **Screen size** | Recommended minimum screen size is 9.7 inches or larger.<br>Small screens that cannot be use for classroom activities are not acceptable. |
| **Operating System** | Microsoft Windows 10 build 22H2 or later.<br>Apple Mac OS X 10.6 or later. |
| **Wireless** | All device must have **802.11x** support, with the ability to connect using **WPA2 Enterprise** encryption.<br>All device must have standard wireless transmission on either the **2.4GHz** bands or higher.<br>Performance will be best on the 802.11n 5GHz band. |
| **Battery Life** | Devices must be fully charged overnight. |
| **Size and Weight** | There is no requirement as such but the device should be of reasonable size to be easily placed on a student's desk and light enough to carry easily. |

## Software

AISC BYOD requires following applications. Users may have additional applications as per their own requirements on their devices.

| | |
|---|---|
| **Web browser** | Firefox version 101 or above.<br>Microsoft Edge Chrome |
| **Security** | Anti-virus, anti-spyware and anti-malware should be installed and updated. AICS uses Malwarebytes but any equivalent software is fine. |
| **Office Application suite** | Microsoft Office 365 suite. AICS has Office 365 licence for all its students. |
| **Adobe Creative Cloud** | AICS has Adobe Creative Cloud licence for all its students (High School Students Only) |
| **LEGO education Spike App** | Can be downloaded free from the internet<br>https://education.lego.com/en-au/downloads/spike-app/software |