



**Al Mawakeb**  
**Bring Your Own Device (BYOD) Agreement**  
**Staff**

**2023-2024**

## Table of Contents

Overview .....	3
Device Options .....	3
Device Usage Guidelines .....	3
Network Connection .....	3
Appropriate Use .....	3
Managing files and saving the work .....	4
Device Security .....	4
Device Care .....	4
Netiquette .....	4
Cyberbullying .....	5
Personal Safety .....	5
Privacy Policy .....	5

## Overview

Al Mawakeb staff members are allowed to bring their own devices, Mobiles, tablets and/or laptop computers, to school and to connect to the school Wi-Fi to gain free limited access to the school network and the Internet. Staff members must read and agree to the guidelines set forth in this document prior to being granted this access. Usage of the above-described devices is solely for educational purposes to fulfil the schools' requirements.

Unless stated otherwise, the guidelines, procedures, and information in this document apply to all devices used by the Al Mawakeb staff members while on school premises.

The staff member is responsible for the safety, security, loss, or damage of their device. While the school takes no responsibility for the staff member's devices, it will make reasonable efforts to support all staff while on-premises.

## Device Options

The school is device brand neutral, however, MacOS devices will have restricted access to the school network. Staff devices must be safe and convenient to use in school.

The staff member is responsible for his/her device at all times. Al Mawakeb takes no responsibility for lost, stolen, or damaged devices.

Every staff member is assigned an Office 365 suite license. It includes Word, PowerPoint, Excel, Outlook, OneNote, MS Teams, and a 1 TB OneDrive cloud storage account.

## Device Usage Guidelines

### Network Connection

Every staff member has access to the school Wi-Fi network and the Internet, can connect to a specified number of devices with limited speed and bandwidth quota. Group Network permissions are position and need based. Devices include mobile devices (smartphones, tablets, e-readers) and laptops.

Upon detection of suspicious activity on/from a device, the IT staff may request an in-person inspection in the presence of the owner.

Any device requiring access to the school's systems such as iCampus, Printers, etc. must have a predefined set of security software installed.

### Appropriate Use

The staff member is responsible for the appropriate use of their device(s) and the installed apps while at school in accordance with the school's Acceptable Use Policy.

Inappropriate usage will result in a disciplinary action.

Staff members are not allowed to:

- Record, film or photograph another staff member / student without asking permission

- Access inappropriate material or an unauthorized App  
Such actions are not tolerated and may result in a disciplinary action.

Inappropriate media may not be used as a screensaver or background photo.

#### Managing files and saving the work

Staff members must use their Microsoft's Office 365 account when saving their school related work. This enables staff members to share and collaborate on a range of documents and is accessible from anywhere and from any device. Every staff member's account has a 1TB OneDrive cloud storage. Office 365 and OneDrive can be accessed using the staff member's email ID.

Staff members should not allow others to access their device and are expected to store their work safely and to back-up important files regularly.

#### Device Security

Staff members must set a pin code/password on their device for security purposes and should not share it with others.

Staff members must have the latest security and operating system patch installed on their device.

#### Device Care

Staff members are responsible to fix and maintain their devices. The school is not responsible to provide a replacement device during the time of the repair; however, the school will make reasonable efforts to support the staff members during such times.

Each staff member is responsible for their own device and should use it responsibly and appropriately. Al Mawakeb takes no responsibility for stolen, lost, or damaged devices, including lost or corrupted data on those devices.

#### Netiquette

Internet access is available to all staff, and we believe these communication links offer vast, diverse, and unique resources. Expected standards of conduct include, but are not limited, to:

- Acknowledging that the access to the Internet is a privilege and not a right
- Respecting the use of copy written materials and the copyright law
- Respecting the rights and privacy of others
- Complying with legal restrictions regarding plagiarism
- Using the school e-mail for professional and not for personal conversations
- Refraining from downloading unauthorized programs and apps
- Refraining from downloading/circulating prohibited media
- Refraining from compromising the security of the school
- Refraining from using the school network and equipment for personal use and private gain
- Respecting the values and ethics of the local culture

## Cyberbullying

Cyberbullying is the use of information and communication technologies to support deliberate, repeated, and hostile behaviour, by an individual or group, in the intent to harm others.

Staff will be held accountable for cyberbullying at Al Mawakeb and will result in a disciplinary action.

Staff members:

- Can disagree with someone else's opinions, however, in a respectful way. *What is inappropriate in the school is inappropriate online*
- Must speak to his/her direct supervisor immediately if they believe someone is a victim of cyberbullying
- Should not answer abusive messages but must report them
- Should not delete anything until it is shown to and documented by his/her direct supervisor at Al Mawakeb (even if it is upsetting, the material is important evidence which may need to be used later as proof of cyberbullying)
- Should not give out their personal details (including usernames and passwords)
- Should never reply to abusive e-mails or messages on any social media platform

Note: All users must read, understand, and abide by the UAE Cyber Law.

<https://u.ae/en/resources/laws>

## Personal Safety

Staff members should always safeguard their personal details/information and should not share it.

Any staff member who feels intimidated, uncomfortable, harassed, or threatened in any way should report the incident to their direct supervisor.

## Privacy Policy

Please read and acknowledge the Al Mawakeb Privacy Policy: <https://almawakeb.sch.ae/privacy-policy>

By acknowledging this agreement, I understand and will abide by the above stated procedures and guidelines. I further understand that any violation is unethical and may result in the loss of my network and/or device privileges as well as other disciplinary action.

I have read the Al Mawakeb BYOD and Acceptable Use Policy and hereby agree to adhere to the guidelines and conditions of use stated within.

I understand that non-compliance with this agreement may result in revoking the privilege of using devices at Al Mawakeb at any time.

I understand that any violation of this agreement including Cyberbullying, will result in the limitation or withdrawal from the BYOD program.

I understand that some rules and guidelines may be changed during the academic year and agree to visit the online copy to get the latest information.

I understand that if this agreement is not acknowledged, I will not be able to connect to the school's network.