WM COLLEGE

INSPIRING LEARNING
SINCE 1854

BYOD
(Bring Your Own Device) Guidelines
2022/23

Created by	David Barnes (Network Manager)
Date of next review	June 2024

Contents

Mobile Device Computing Guidelines 3
Purpose 3
Scope 3
Exceptions 3
Details 3
Requirements for Users 3
Requirements for the IT Department 6
Acknowledgment of Mobile Device Computing Guidelines 7
Procedure 7
Signature 7

Mobile Device Computing Guidelines

Mobile devices are a way of life, in the consumer, business and education realms—and business interests must be protected where the two converge. The, bring your own device (BYOD) approach, which allows Staff and learners to use their own mobile devices to perform college business, like connecting to email and cloud services, is accepted by a majority of organisations now. Mobility in business terms means being able to get the job done and stay connected regardless of location, device, or time of day.

However, the convenience of mobile computing also has a price tag in the form of added security management and the necessity of allowing IT control over devices to ensure that the college, its personnel, and its data remain protected. These details can be complicated—and the costs incalculable if they are not properly addressed.

Purpose

This document provides guidelines for the safe and productive use of mobile devices (laptop computers, tablets, smartphones, etc.) by staff and learners. It includes requirements for users and requirements for IT departments responsible for supporting and administering mobile devices.

Scope

This document is intended to support staff, learners, guests and any contractors using devices in the college, It applies to all college-owned equipment and related material, as well as staff / learner-owned devices used to connect to the colleges systems as part of a BYOD arrangement.

Exceptions

There are no exceptions to this document unless permitted in writing by the IT department or personnel authorised to make such decisions.

Details

Staff must be approved to receive mobile devices paid for by the college as part of their job duties. This approval should be made by managers during the hiring process and communicated to IT / Finance and HR to arrange procurement of the device(s).

Requirements for Users

- Ensure that all mobile device use is for business / professional reasons. Only access information that is needed to perform your job or assist others in doing so as part of the valid scope of their duties.
- Do not share devices with other WMC staff or non-college personnel.

- Never share private passwords with those who are not authorised to have them or leave passwords in an accessible place (such as on a post-it note). Passwords must be changed immediately if you suspect they may have become known to others.
- Store all shared mobile device passwords (such as for loaner equipment) in a centralised and encrypted password database. The main password for these databases must also be kept private and provided only to authorised staff.
- Do not use unsecured networks (wired or wireless). If possible, arrange for a portable Mi-Fi or tethering via a device equipped with internet access so you can avoid using unknown networks.
- Do not install unauthorised or pirated applications.
- Install only software that is college owned and / or authorised for use by the IT department.
- Download files only from known good sources for business purposes. All systems handling these files must have updated anti-malware programs, which must not be disabled or tampered with.
- If applicable, run a virus scan on any executable file(s) received through the internet. If a virus is found (either during a scan or via a check by anti-malware software, power off the system and immediately contact the IT department to notify them of the situation; take no further action until instructed.
- Do not access or view confidential or copyrighted material if you are not authorised to do so. Do not copy or transfer copyrighted materials without permission.
- Know and abide by all applicable college policies dealing with security and confidentiality of company records.
- Avoid transmission of private or confidential information via mobile devices. If it is necessary to transmit this data, take steps reasonably intended to ensure that information is delivered to the proper person who is authorised to receive such information for a legitimate use.
- Share and store private or confidential information by adhering to security restrictions (e.g., via encrypted transmission or encrypted media). For instance, do not keep private or confidential information on unsecured media or staff-owned or unsecured devices, such as flash drives or laptops, or staff-owned cloud storage applications.
- No single copy of college data is to be stored on any mobile device—secondary copies must be kept on an internal server.
- No learner / staff data, such as social security numbers, driver's license numbers, and bank / credit card numbers, should be kept on mobile devices.

- All laptops must have antivirus / firewall protection and current application / operating system patches installed.
- These applications / settings / procedures should not be tampered with or circumvented.
- Never access, insert, or connect to college systems any disks, USB drives, or other storage media of unknown origin.
- Arrange for a locked case to carry mobile devices. Laptops must be stored in locked cases while in transit.
- Mobile devices are to be kept under your control at all times. Do not check, ship, or give them to anyone else for transport.
- Keep in mind that airports, train stations, bus terminals, and other high-traffic travel areas can be particularly dangerous places in terms of loss or theft. Exercise special caution in these areas.
- It is acceptable for security personnel to x-ray mobile devices. However, metal detectors can harm these objects, so travellers should request visual inspections instead.
- Do not leave mobile devices visible in unattended vehicles, even if locked.
- Do not leave mobile devices unprotected in hotel rooms—use a safe or a security cable.
- If possible, copy any updated company information on a mobile device back to internal servers periodically via secure means, such as VPN connections.
- Notify your manager as well as the IT department immediately if a device is lost or stolen.
- If using BYOD, consult the manufacturer / vendor / carrier for support of your device before requesting assistance from the company IT department.
- In the event that you believe a personally owned or college-provided device authorised to connect to the organization’s resources, systems, and networks might be infected by a malware threat or might be somehow compromised, you must immediately notify the IT department, by phone, email or in person, of the potential security risk.
- In the event that you lose or misplace a personally owned or college-provided device authorised to connect to the college’s resources, systems, and networks, you must immediately notify the IT department, by phone, email or in person, of the potential security risk.
- Do not discard previously authorised devices until the IT department approves the device for disposal.

- Whenever you decommission, prepare to return, or otherwise cease using a personally owned or college provided device authorised for business use, notify the IT department that the device will no longer be used to connect to college's resources, systems, and networks.
- Hand in all college-issued systems and devices upon termination of employment.
- Submit any employee-owned systems or devices that have accessed company resources to the IT department for inspection upon termination or when the system / device no longer requires this access.
- Notify the IT department of all passwords, the whereabouts of any confidential data, and any other details that should be transferred to others upon termination of employment.
- Be aware that the IT department reserves the right (and will proceed) too remotely wipe a device if it has been lost or you have been terminated and have not brought the device to the IT department for decommissioning.

Requirements for the IT Department

- If applicable, the IT department should have a procurement and support policy for issuing college-owned mobile devices. Standardise on the smallest number of models possible for consistency of use and ease of support.
- Where possible, the IT department should apply centralised security policies (such as via a Mobile Device Management platform, ie Microsoft Intune) to college-connected mobile devices. These policies should enforce a password / biometric policy that will automatically lock the device after a one-minute period of inactivity and erase the contents of memory and storage after a maximum of 10 failed authentication attempts. Password changes should be enforced on connected devices. The policy should also include the ability to remotely erase (wipe) these devices of commpany data in the event of loss or theft.
- If such a college-wide policy does not exist, screen lock / password settings should be individually applied.
- Implement and support secure remote connectivity methods for mobile devices to access company resources, such as via an encrypted VPN connection or fully secured Remote Desktop.
- Ensure that all mobile devices run anti-malware / virus software that is updated regularly and confirm that all critical and security patches are installed on mobile devices on a periodic basis.

- Facilitate the use of shared password databases, security cables, and portable hotspots, such as Mi-Fi equipment for users if required.
- Develop a written plan to handle malware infections, lost or stolen devices, and device decommissioning and replacement procedures.
- Establish an on-call or after-hours method for users to communicate device mishaps, such as theft or malware infection.
- Enforce encrypted storage mechanisms on mobile devices if the potential exists for the device to save, cache, or even temporarily store organisation data. This should entail at minimum 128-bit encrypted storage (AES is recommended). This includes external USB flash drives and internal storage cards. Where possible, whole disk encryption should be employed.
- When a mobile device is to be decommissioned, remove any required encryption, VPN, and antimalware licensing from the user's device. Also confirm that the user's device does not contain any traces of protected, sensitive, corporate, or proprietary information and delete any such data remaining on the device.
- Remotely wipe a device if it has been lost or the employee has been terminated and has not brought their device to the IT department for decommissioning.

Acknowledgment of Mobile Device Computing Guidelines

This form is used to acknowledge receipt of and compliance with the company's Mobile Device Computing guidelines.

Procedure

Complete the following steps:

1. Read the Mobile Device Computing guidelines.
2. Sign and date in the spaces provided.
3. Return a copy of this signed document to the Human Resources (HR) department.

Signature

Your signature attests that you agree to the following terms:

I. I have received and read a copy of the Mobile Device Computing guidelines and I understand and agree to the same.

II. I understand the organisation may monitor the implementation of and adherence to these guidelines to review the results.

III. I understand that violations of the Mobile Device Computing guidelines could result in termination of my employment and legal action against me.

______________________________ ______________________________

Employee Full Name ***Employee Title***

____

Department / Location

______________________________ ______________________________

Employee Signature ***Date***