	UWC		
UNIVERSITY of the WESTERN CAPE	**Bring Your Own Device (BYOD) Policy**	Council Approval Reference Number	C2021/03 (29 June 2021)
		Implementation Date	1 July 2021
		Revision / Amendment	ICS
		Revision / Amendment Date	09 June 2021
		Policy Owner	UWC ICS
		Executive Management Portfolio	ED – Finance and Services
		Contributors	ICS
		Circulated by:	ICS
		Circulated to:	ED – Finance and Services ICS Management EMC

UNIVERSITY OF THE WESTERN CAPE (UWC)

BRING YOUR OWN DEVICE (BYOD) POLICY

(USE OF PERSONALLY OWNED DEVICES AT THE UNIVERSITY)

DATE OF LAST APPROVAL: C2021/03 (29 JUNE 2021)

Contents

Last Update Status: *Updated June, 2021*

1. Overview

Rapid advancement of technologies for mobile devices such as smartphones, tablets, laptops, and internet ready wearable devices encourage users to use their personal devices at their places of study and work. Bring Your Own Devices (BYOD) phenomenon is now becoming pervasive and highly demanding for enhancing learning and teaching experiences.

The main concern for BYOD implementation in the campus environment is the accessibility of the internet resources for BYOD users to ensure they can complete their tasks accordingly. At the same time, universities must protect IT infrastructure and data while users are given access privilege to the campus network and information systems.

The University is moving toward a Flexible Learning and Teaching model. In order to ensure that students are able to actively participate in this model, the implementation of a BYOD policy is geared at allowing the flexibility for students to primarily use their own devices.

Please note that the University reserves the right to refuse, prevent or withdraw access to users and/or devices or software where it considers that there are unacceptable security or other risks, to its staff, students, business, reputation, services or infrastructure. BYOD users must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the UWC network.

This policy sets out the minimum requirements.

2. Purpose

The purpose of this policy is to provide a consistent and secure approach for the acceptable use of personally-owned devices that access UWC systems.
The aim of the policy is to ensure that the University complies with data protection legislation and that University information, in particular personal and sensitive information, is protected from unauthorised access, dissemination, alteration or deletion and that University data, applications, services, the academic program and University operations remain available when needed.

3. Scope

This policy applies to all University staff, Council members, students, vendors, contractors and visitors that access or process University data on personally owned devices. The term for such devices is BYOD ("bring your own device").

This policy also applies to using personal devices for study and work purposes off the University premises. If you are using your own device, you have a responsibility to configure it securely.

Where students are unable to furnish their own laptop devices, the University may facilitate the sourcing of laptop devices.

Exclusions:

Any UWC departments that are required to work with sensitive and proprietary data is not eligible to use their own Personal Computer devices.

4. Definitions

Acceptable use

Refers to the responsible, ethical and lawful use of ICT resources in accordance with the Acceptable Use Policy and applicable laws and regulations to prevent any reputational damage, legal liability or risk to UWC.

Anti-virus

Software designed to detect and remove viruses from a computer.

BYOD

The practice of allowing employees of an organisation to use their own computers, smart phones or other devices for work purposes.

Confidential data

Information and related IT Resources whose unauthorized disclosure or modification could result in small to moderate fines, penalties or civil actions. Institutional Information of which unauthorized use, access, disclosure, acquisition, modification, loss or deletion could result in moderate damage to UWC, its students, patients, research subjects, employees, community and/or reputation related to a breach or compromise; could have a moderate impact on the privacy of a group; could result in moderate financial loss (between R100k – R500k); or could require legal action. This classification level also includes lower risk items that, when combined, represent increased risk.

Denial of Service Attack (DoS)

An assault on a service from a single source that floods it with so many requests that it becomes overwhelmed and is either stopped completely or operates at a significantly reduced rate.

Encryption

Encryption is the process of converting data to an unrecognizable or "encrypted" form. It is commonly used to protect sensitive information so that only authorized parties can view it. This includes files and storage devices, as well as data transferred over wireless networks and the Internet.

Information asset

Any information or data that is of value to UWC whether in electronic or hard copy format and if its security is compromised, it would have a significant impact on the institution's business operations.

IT

The Information Technology (IT) department that is responsible for delivering Information and Communication Technology (ICT) services to the UWC community.

Malware

Short for malicious software designed to infiltrate, damage or obtain information from a computer system without the owner's consent. Malware is commonly taken to include computer viruses, worms, Trojan horses and spyware.

Sensitive data

Any information protected by national or local laws and regulations, or industry standards such as GDPR, POPIA, PCI-DSS. Institutional Information and related IT Resources whose unauthorised disclosure or modification could result in significant fines (>R500k), penalties, regulatory action, or civil or criminal violations. Legislative, regulatory and contract obligations are major drivers for this risk level. Other drivers include, but are not limited to: the risk of significant harm or impairment to UWC students, patients, research subjects, employees, guests/program participants; UWC reputation related to a breach or compromise, the overall operation of the Location or essential services.

User

Any person (e.g. UWC student, staff, third party, etc.) who has been authorised to access UWC's information assets and related systems.

5. Policy

5.1 Policy Agreement

5.1.1 All employees and students using devices falling into the category “BYOD” devices must acknowledged that they have read and understood this security policy and the associated procedures before they are allowed to access UWC services using their personal devices.

5.2 Student devices

5.2.1 Students are encouraged to provide their own devices. Where required, the University may facilitate the sourcing of laptop devices.

5.2.2 Students are required to maintain their own devices.

5.3 Acceptable Use

5.3.1 The BYOD User is expected to use his or her devices in an ethical manner at all times and adhere to the company’s *Acceptable Use Policy*.

5.3.2 IT will take reasonable measures to provide institution-wide Information Security awareness and implement appropriate safeguards to protect information assets however users must ensure that they use the information assets securely and responsibly as prescribed in the *Acceptable Use Policy*.

5.4 Devices and Support

5.4.1 Connectivity issues are supported by the UWC IT Department.

5.4.2 Sensitive and UWC-confidential documents must never be stored on personal devices.

5.4.3 Devices connecting to the UWC wireless network must support the 802.11ac wireless protocol standards to maximize their WIFI connectivity experience.

5.4.4 Devices connecting to the UWC wireless network must support the 802.1x wireless authentication protocols.

5.5 Information Security

5.5.1 In order to prevent unauthorised access, devices must be password protected using the features of the device and a strong password (**Please refer to the UWC Password Policy**) is required to access the University’s network.

5.5.2 Leaving your device unattended while logged onto the University systems or network will be deemed a breach of this policy.

5.5.3 University data should only be downloaded to your personal devices if it is personal to the user downloading it. If you are in any doubt as to whether particular data can be stored on your device, consult with your manager, or seek advice from UWC IT Service Desk or from the University Registrar's Office.

5.5.4 Hard disk, mobile phone and data transmission encryption should be enabled where possible.

5.6 Monitoring of User-Owned Devices

5.6.1 The University will not monitor the content of your personal devices, however the University reserves the right to monitor and log data traffic transferred between your device and University systems, both over internal networks and entering the University via the Internet.

5.7 Risks/Liabilities/Disclaimers

5.7.1 It is the BYOD User's responsibility to take additional precautions, such as backing up email, contacts, etc.

5.7.2 The University reserves the right to disconnect devices or disable services without notification.

5.7.3 The loss, theft or misuse of a user device is personally distressing. If you use sensitive data, it can also have serious consequences for others, for example staff and students about whom information is held. In addition, there may be significant legal, financial and reputational consequences for the University. Lost or stolen devices must be reported to the IT department or Service Desk and logged as an incident **AS SOON AS IT IS NOTICED**. Employees and students are responsible for notifying their mobile carrier immediately upon loss of a device.

5.7.4 The BYOD User is personally liable for all costs associated with his or her device.

5.7.5 The BYOD User is solely responsible for the cost of maintenance.

5.7.6 The BYOD User assumes full liability for risks including, but not limited to, the partial or complete loss of University and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

6. Policy Compliance

Some of the scenarios that will constitute a failure to comply with this policy are listed below:

Information Security Data Breach using BYOD device i.e. UWC network accessed and data is lost through the use of a BYOD device where the user is shown to have been grossly negligent with respect to the compliance to this policy.

Denial of Service Attack using a BYOD device i.e. UWC system downtime experienced as a result of a security breach via a BYOD device where the user is shown to have been grossly negligent with respect to the compliance to this policy.

Loss of Confidential Information from a BYOD device i.e. UWC confidential information lost as a result of the theft or loss of a BYOD device where the user is shown to have been grossly negligent with respect to the compliance to this policy.

Compliance Measurement

The Information Security team will verify compliance to this policy through various methods, including the Root Cause Analysis of data related incidents, Network Monitoring reports and logs, internal and external audits, and feedback to the policy owner.

Non-Compliance

A BYOD User found to have breached this policy may be subject to the University Code of Conduct and HR Disciplinary Processes.

7. Roles & responsibilities

- BYOD Users are required to act in the best interest of UWC, its assets and its services.
- In case of doubt, BYOD Users must contact the UWC IT department to clarify a given situation.
- BYOD Users must diligently protect such devices from loss and disclosure of private information belonging to or maintained by UWC.
- The UWC IT Service Desk must be notified immediately upon suspicion of a security incident, especially when a mobile device may have been lost or stolen.
- UWC IT is responsible for developing procedures for implementing this policy.
- This policy should be reviewed by UWC IT on a regular basis or with changes to regulations and legislation.

8. Related Standards, Policies and Processes

- Password Policy (C2005/3)
- Acceptable Use Policy (C2021/03)
- Information Security Policy (C2021/03)
- Code of Conduct
- HR Disciplinary Process

9. Revision History

Date of Change	Responsible	Summary of Change
21 October 2020	ICS Director	Document Creation
04 February 2021	Gail Francke	• Added statement 5.3.2 from the Acceptable Use Policy to ensure referencing to information protection in this BYOD policy • Added the minimum device requirements 5.4.3 and 5.4.4 • Added 'Information' to heading 5.5 to read 'Information Security' • Added definitions: Acceptable Use, IT, Information asset, User
09 June 2021	Gail Francke	• Updated the Scope last paragraph to replace the word 'require' with 'encourage' students to furnish their own devices. • Updated 5.2.1 to replace the word 'require' with 'encourage' students to furnish their own devices. • Split 5.2.1 to add 5.2.2 as students are required to maintain their own devices. • Replaced the word 'secret' with 'sensitive' in 5.4.2 • Added 'Sensitive data' and 'Confidential data' definitions to 4. Definitions