University of South Wales
Prifysgol De Cymru

Mobile Device Policy

DOCUMENT CLASSIFICATION	[PUBLIC / CYHOEDDUS]
DOCUMENT REF	USW-ISMS-DOC-A06-EN
VERSION	1.0
DATED	20 April 2022
DOCUMENT AUTHOR	Ryan Olden – End User Compute Manager
DOCUMENT OWNER	Ian Anderson – Head of Core Technology Services
REVIEW BY DATE	20 April 2024

Revision history

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
0.1	24 JAN 2022	Jon Phillips	Initial Draft
0.2	14 FEB 2022	Ryan Olden	ITS Approval Review
1.0	20 APR 2022	Ross Davies	ISSG Approval

Approval

NAME	POSITION	DATE
Paul Harrison	Chair of ISSG	20 APR 2022

Contents

1 Introduction

Mobile computing is an increasing part of everyday life, as devices become smaller and more powerful the number of tasks that can be achieved away from the office grows, enabling greater flexibility. However, as the capabilities increase so do the risks. Security controls that have evolved to protect the static desktop environment are easily bypassed when using a mobile device outside of the confines of on-campus infrastructure.

Mobile devices include items such as:

- Laptops
- Notebooks
- Tablet devices
- Smartphones
- Smart watches

Mobile devices are used to access USW systems and are capable of storing and processing USW data. These include, but are not limited to Email, Office files, HR Employee Self Service (ESS) and the Student Records System.

1.1 Scope Statement

The purpose of this policy is to set out the controls that must be in place when using mobile devices. It is intended to mitigate the following risks:

- Loss or theft of mobile devices, including the data on them
- Compromise of classified information.
- Introduction of viruses and malware to the network
- Loss of reputation

It is important that the controls set out in this policy are always observed in the use, transport, and administration of mobile devices.

This policy applies to all systems, people and processes that constitute the information systems, including colleagues[1], students, governors, suppliers, contractors and other third parties [2]who have access to the University of South Wales systems via a mobile device.

The University's Information Management Policy contains details of the restrictions and practices required to protect information being stored and processed on mobile devices. These restrictions and practices depend on the classification of the information and must be followed.

[1] Including colleagues from, USW, PSS and USW Pathway College Ltd
[2] Including USWSU

1.2 Roles & Responsibilities

IT Services Information Security Team: ensures appropriate precautionary measures (both technical and process-wise) are established and maintained. The team is actively involved in identifying security loopholes and handling incidents that could result in system compromise and the loss of protected (non-public) information.

University Secretary's Office Information Compliance Unit: responsible for USW's information classification scheme and setting what classification(s) of data can be accessed via mobile devices and any additional controls required.

IT Services End User Computer Team: responsible for the secure configuration and administration of all mobile devices used to access USW systems, infrastructure, and data.

IT Service Desk: responsible for providing end-user guidance and assistance to queries and issues in respect of their compliance to this policy.

End-users: It is the responsibility of every colleague and user covered by the scope of this policy to use mobile devices in accordance with it. This will apply to user-owned "Bring Your Own Device" (BYOD) assets if they are used to access USW systems, infrastructure, and data.

2 Devices Provided by the University

2.1 End-Users

This policy section sets out requirements on colleagues, students, and other end users who have been granted access to a USW mobile device.

If you are authorised to make use of university mobile equipment, you will be provided with an appropriate device which will be configured to comply with the university's policies.

The university typically provisions devices with standard configurations and sets of capabilities based on generic requirements. These should enable adequate functionality across a range of use cases and offer choice and flexibility to meet the needs of a diverse user base. Users with specific device and software requirements to improve accessibility (related to protected characteristics) should bring these to the attention of IT Services to determine the nature of any reasonable adjustments.

Support will be provided by IT Services who may at times need access to your device for problem investigation, resolution and maintenance purposes.

You must ensure that the device is transported in a protective case when possible and is not exposed to situations in which it may become damaged. Do not leave the device unattended in public view, such as in the back seat of a car or in a lecture room or canteen. Do not leave the device in an open or other unsecured location.

Do not remove any identifying marks on the device such as a USW asset tag or serial number. Ensure that the device is locked away when being stored and that the key is not easily accessible.

Do not add peripheral hardware other than:

- USW Equipment provided with the device (e.g. docks);
- Input devices such as mice and keyboards;
- Monitors; and
- Headsets, speakers, and microphones

to the device without the approval of IT Services.

Do not keep anything with the device that may allow someone to gain access to it. For example, a provided hardware access token.

Ensure that the device screen locks after a short period of not being used and requires an approved authentication method to unlock it. See the Access Control Policy for details of acceptable password characteristics and other approved authentication mechanisms.

The USW-provided device is for your use in relation to university or academic activity; it must not be shared with family or friends. You should only use provided devices for university-related purposes such as teaching and learning activities or to support your job role. However, the university allows limited personal use, in line with the current IT Computing Regulations. Colleagues should be aware that their USW device will be monitored in line with the Logging and Monitoring Policy. You may be asked to return the device to IT Services at any time for inspection and audit. You must not attempt to install any unauthorised software or change the configuration or setup of the device without consulting IT Services first.

Where possible, the device will be secured so that all the data on it is encrypted and so is only accessible to authorised users. If the device is supplied with encryption, do not attempt to disable it.

Files held on the device are not necessarily subject to USW backup mechanisms. Store any files you consider important on the University's cloud storage platform. Do not take your own unencrypted backups of classified information.

Where applicable, malware protection will be installed on the device by the university. Ensure that the device is connected to the Internet on a regular basis to allow the anti-malware software to update itself to ensure the device is protected against the latest threats. Do not attempt to disable virus protection on the device.

You must only connect the device to non-USW networks you reasonably trust such as your home wireless network. If you need to connect to non-USW public networks and your device has been configured to use the USW VPN, you should consider utilising the USW VPN. This protects the data flow to/from your device.

When connected to the USW VPN you must not allow your device to be “tethered” to another in such a way that your device acts as a bridge between the USW network and other unauthorised devices.

When in public places, ensure that you site the device such that unauthorised people cannot view (or take photographs or video of) the screen.

The user must notify Information Security (via IT Support) if they notice any confidential information missing from the device.

If the user loses the device or in case of theft of the device, it is the user's responsibility to notify IT Services immediately as well as log a lost/theft complaint with the local law enforcement agency.

If for any reason, there is a regulatory or legal requirement to examine the device, the user is expected to surrender the device. Where circumstances allow, this should be with the knowledge and assistance of the Head of Information Security or delegated person.

2.2 Device administration

This policy section concerns colleagues responsible for the administration of USW mobile devices. Devices must only be administered by colleagues who are authorised and competent to do so.

Mobile devices must be configuration hardened and security patched in accordance with the Technical Vulnerability Management Policy.

A mechanism should be put in place to allow for the remote triggering of security updates.

Administrators should assume that the devices they manage have the potential to access, store and process USW CONFIDENTIAL classified information and must therefore leverage aspects of the device and operating system to provide appropriate defence in depth technical controls.

All mobile devices must be configured with encrypted storage to protect data at rest.

IT Services are responsible for ensuring any required vulnerability scans are conducted against the device.

Where end-users are exceptionally granted administrative privileges on a device they must not attempt to disable or circumvent software, on-device policies, control mechanisms or anything that has been provisioned in relation to the security posture of the device.

3 Use of Personally Owned Mobile Devices

This section explicitly excludes devices belonging to students, suppliers and third-parties. Information for students relating to acceptable use of their own IT equipment, particularly when connected to USW resources are contained within the current Student Code of Conduct and IT Computing Regulations.

USW data and systems must not be accessed from public / shared user devices, for example in public libraries.

This policy section concerns the use of mobile devices that are personally owned by colleagues and governors, when used to access USW systems and information requiring authentication of their IT account. This includes accessing work email and the USW collaboration platform but exempts accessing publicly available information presented on the USW websites.

Visitors to the university, such as guest lecturers, should use their own devices to connect to the appropriate USW guest network.

The low cost and general availability of such devices has fuelled the desire amongst colleagues and other stakeholders to use their own devices for university use. This is commonly referred to as “Bring Your Own Device” (BYOD). In some cases, this can provide increased flexibility around working and necessitate diversity and inclusion in the workforce.

However, the concept of allowing a colleague to make use of their own device(s) for university purposes may result in the need for such devices to be subject to additional controls over and above those typically in place for a consumer device.

Common issues and security challenges with BYOD may include:

- Use of the device by other family members
- Default storage of data in cloud backup facilities
- Increased exposure to potential device loss in social situations e.g. on the beach, in a bar
- Potential access to websites that do not meet the university’s acceptable use / filtering policies
- Connection to insecure networks e.g. unsecured wireless hotspots
- Anti-virus protection and how often the device is patched
- Installation of potentially malicious apps onto the device (often without the user being aware that they are malicious)

These issues must be considered when assessing the suitability of any given device to hold specific data belonging to the university.

Use of any suitable BYOD device for work purposes is not compulsory. Colleagues must personally assess whether the additional controls placed on their device by the university are acceptably balanced with the increased convenience and flexibility their use can offer.

The University has the right to determine whether a particular device is suitable, i.e. meets the standards with respect to being capable of mitigating current threats to information security. The University reserves the right to immediately and irrevocably deny access to USW systems and data to any device that is determined not to meet the current standard. An example of this may be because the device or its operating system becomes no longer supported by the vendor.

The user may be asked to install or configure specific apps, software, platforms or features to their devices to enable them to be authorised to access USW systems, services, and data. Any such request must be complied with whilst such access is required.

The user is expected to update their device as soon as reasonably practicable as new operating system and security patches become available to maintain the security of the device. A device that is not updated with these patches might be de-authorised as it is more vulnerable to attacks and hence will put both University and personal information at risk.

The security posture of devices that have been "jail-broken" or "rooted"[3] cannot be assured therefore they must not be used to access USW systems, services, and data.

The user must comply with any reasonable request to assist with any USW IT security incident investigation that may concern their BYOD device.

In the event of the BYOD device being lost or stolen, the owner must inform IT Services as soon as possible, giving details of the circumstances of the loss and the sensitivity of the university information stored on it. The University of South Wales reserves the right to remotely wipe the device where possible as a security precaution. This may involve the deletion of non-university data belonging to the device owner.

If you are selling or otherwise disposing of a device that has previously been configured to access USW data, then you must disconnect this device from USW following our guidelines on Device removal to ensure university data and applications are safely removed.

Upon leaving the organisation, the device owner must allow the device to be audited and all university-related data and applications must be removed.

3.1 USW Administration of a Personally Owned BYOD Device

This policy section concerns colleagues responsible for the administration of BYOD mobile devices.

It is recognised that the diverse characteristics of mobile devices mean that each platform (Android, iOS, Windows etc.) will have unique capabilities and requirements concerning the extent to which a given platform is managed and the mechanism(s) for doing so. Separate procedures should be determined to deliver an appropriate security posture for each supported platform. The IT Services End User Compute team, supported where appropriate

[3] Jail-broken or rooted relates to modifying a smartphone or other electronic device to remove restrictions imposed by the manufacturer or operator, e.g., to allow the installation of unauthorised software.

by the Information Security team, are responsible for determining and deploying adequate configurations.

Configuration policies for BYOD devices and/or applications accessing university data must be managed and deployed via a USW mobile device management system.

Mobile device management systems should be capable of inventorying each device and recording vendor, model, operating system, and installed software.

Administrators should assume that the BYOD devices have the potential to access, store and process USW CONFIDENTIAL classified information and must therefore leverage aspects of the device and operating system to provide appropriate defence in depth technical controls.

Mechanisms such as Conditional Access Policies must be in place to reject requests from devices whose posture fall below the current security standard. Such mechanisms should be applicable to third-party devices connecting to USW systems.

4 ISMS Conformance

4.1 Areas of ISO/IEC 27001:2013 addressed

The following areas of the ISO/IEC 27001:2013 standard are addressed by this document:

- A.5 Information security policies
  - A.5.1 Management direction for information security
    - A.5.1.1 Policies for information security
- A.6 Organization of information security
  - A.6.2 Mobile devices and teleworking
    - A.6.2.1 Mobile device policy
- A.11 Physical and environmental security
  - A.11.2 Equipment
    - A.11.2.6 Security of equipment and assets off-premises

4.2 Related Policies and Regulations

The following policies and procedures are relevant to this document:

- *Access Control Policy*
- *Software Policy*
- *Teleworking Policy*
- *User Access Management Process*
- *Technical Vulnerability Management Policy*
- *Information Management Policy*

- *Data Breach Procedure*
- *USW IT Regulations*
- *Student Code of Conduct*