Bring Your Own Device (BYOD) Policy (ISP-13)

Document Owner

Executive Owner:	Darrell Morrison
Functional Area:	Information Technology

Authorization

Authorized By:	David J. Hinson
Position:	Interim Chief Information Officer
Signature	
Authorization Date	02/25/2025

Version History

Issue	Reason For Change	Date
1.0	Initial Release	02/25/2025

Review Period

Information Security Policies are to be reviewed at a minimum annually.

Change Control

Requests for changes to Information Security Policies are to be sent to the document owner providing details of the requested changes and a short justification.

Exceptions

Requests for exceptions to this policy are to be submitted in accordance with the exception policy. Note that all exceptions are time limited to no more than 12 months in duration.

Applicability

This policy applies to all faculty, staff and contractors who utilize a privately owned device be that a cell phone, tablet, PC or Mac to access University Information Systems.

Table of Contents

Introduction

The use of non-University owned devices to access and process University data can expose that data to a risk of compromise. This can be mitigated by defining and agreeing acceptable User behaviors and implementing a minimum set of security controls that the User agrees to abide by.

Objective

This policy defines Users' responsibility if they utilize a device not provided by the University for accessing, viewing, modifying, and deleting University held data.

Definitions

Bring Your Own Device (BYOD) refers to the use of non-University owned electronic devices to access and store University information. Such devices include smart phones, tablets, laptops, flash drives, and similar technologies, whether onsite or remotely, typically connecting to the University's Wireless Service.

Data Controller: The Data Controller is a person, group, or organization (in this case the University) who determines the purposes for which, and how, any personal data is processed.

Policy Statement

General

If you wish to use a BYOD to access University systems, data, and information, you may do so, if you follow the provisions of this policy subject to the University meeting its legal and duty of care obligations.

The University, as the Data Controller, controls the data regardless of device ownership.

As a User you are required to keep University information and data secure. This applies to information held on your BYOD, as well as on University systems. You are required to assist and support the University in carrying out its legal and operational obligations, including co-operating with the Information Technology Department should it be necessary to access or inspect University data stored on your personal device.

The University reserves the right to refuse, prevent or withdraw access to users and/or devices or software where it considers that there is unacceptable security, or other risks, to its staff, students, business, reputation, systems, or infrastructure.

Conditions of Use

The use of a BYOD device must adhere to the University's Acceptable Use Policy. When you use your own device as a work tool, you must maintain the security of the University's information you handle (which includes but is not limited to viewing, accessing, storing, or otherwise processing data). Sometimes, the University may require that you install or update University-approved device management software on your own device. It is your responsibility to familiarize yourself with the device sufficiently to keep data secure.

In practice this means:

- To prevent theft and loss of data, the device should not be left unattended, and an automated screen lock must be enabled within 5 minutes of inactivity that requires a password and or PIN to unlock.
- Keeping information confidential ensuring Restricted and Confidential data is not placed on USB drives or on private cloud storage solutions. Additionally, you must be aware of others looking at your screen (Shoulder surfing).
- Maintaining the integrity of data and information, most notably ensuring all University data is saved to OneDrive or other University provided cloud storage solution in event the device becomes unusable.
- Keep the device software up to date, for example using Windows Update or Software Update services.
- Activate and use encryption services and anti-virus protection if your device features such services.
- Install and configure tracking and/or wiping services, such as Apple's 'Find My iPhone app,' Androids 'Where's My Droid' or Windows 'Find My Phone,' where the device has this feature.
- Remove any University information stored on your device once you have finished with it including deleting copies of attachments to emails, such as documents, spreadsheets, and data sets.
- Limit the number of emails and other information that you are synchronizing to your device to the minimum required.
- Remove all University information from your device and return it to the manufacturers' settings before you sell, exchange, or dispose of your device.
- If your device is lost or stolen, or its security is compromised, you must promptly report this to the Information Technology Helpdesk, so they may assist you to change the password to all University services. It is also recommended that you do this for any other services that you have accessed via that device, e.g., social networking sites, online banks, online shops.
- You must also cooperate with University officials in wiping the device remotely on loss or compromise, even if such a wipe results in the loss of your own data, such as photos, contacts, and music.

Monitoring of User Owned Devices

The University will not monitor the content of your BYOD device(s); however, the University reserves the right to monitor and log data traffic transferred between your device and University Information Systems, both over internal networks and entering the University via the Internet.

In exceptional circumstances, for instance where the only copy of a University document resides on a personal device, or where the University requires access in order to comply with its legal obligations (e.g. under Open Records Laws, or where obliged to do so by a Court of law or other law enforcement authority) the University will require access to University data and information stored on your personal device. Under these circumstances, all reasonable efforts will be made to ensure that the University does not access your private information.

Support

The University takes no responsibility for supporting, maintaining, repairing, or ensuring BYOD devices, or for any loss or damage resulting from support and advice provided.