Bring Your Own Device

NAME:	Bring Your Own Device
ISSUING DEPARTMENT	Campus Technology
ISSUED DATE:	Provisionally Approved March 17, 2020
REVIEWED DATE:	
APPROVING AUTHORITY:	Cabinet
DATE REVISED:	

INTRODUCTION

Bring your own device (BYOD) is the act of using a personal computing device (computer, tablet, phone, etc.) for work or business related activities. Mansfield University does not **require** employees to use personal equipment for business operations. Those employees who wish to use their personal devices must abide by the policy below. Mansfield University is not responsible for the purchase or costs associated with use of personally owned devices. In response to an increase in personally owned devices being used in the work environment, Mansfield University has established an official Bring Your Own Device (BYOD) policy.

DEFINITIONS

Up-to-date Anti-virus Protection
Virus Protection with definitions that are no more than 10 days old

Personally Identifiable Information
Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Sensitive Information
Any information that can be used to identify you or another person. Examples include: personal information, medical records, financial information, University administrative computer data (employee records, student records, electronic documents that contain confidential information), passwords and account details, and research data.

PURPOSE

This policy defines the appropriate use and procedures for using personally owned computing devices on the Mansfield University network, Physical or Virtual (VPN) and the storage of intellectual property, sensitive data or University licensed software.

PURPOSE

This policy applies to employees, faculty and staff, and any other user that utilizes the network or computing resources provided by Mansfield University for business related activities with a personally owned device such as:

- Portable computers; e.g.; laptops, notebooks, netbooks
- Portable storage media; e.g.; USB storage devices, flash memory cards, CD/DVD ROM
- Mobile devices; e.g.; cellular smartphones, tablet computers

POLICY

Faculty and staff who choose to participate in BYOD must abide by this policy and all University policies while using a personally owned device on the Mansfield University network. Additional key mandatory policies when using personally owned devices include but are not limited to; Acceptable Use Policy, Data Policy and Bandwidth Policy.

All Information Technology policies are available on the Mansfield University Policy and Procedures page, https://www.mansfield.edu/policies-procedures/

Employees who participate in the BYOD policy must:

- Not store Mansfield University Personally Identifiable Information or Sensitive Information on personally owned devices.
- Destroy, remove or return all data, electronic or otherwise belonging to Mansfield University, once their relationship with Mansfield University ends or once they are no longer the owner or primary user of the device. (e.g. the sale or transfer of the device to another person)
- Remove or return all software application licenses belonging to Mansfield University when the device is no longer used for Mansfield University business.
- Notify Campus Technology of any theft or loss of the personal device containing data or software application licenses belonging to Mansfield University.
- At no time may the personal device be connected to the secure Mansfield University networks without prior authorization.
- Employees are expected to refrain from using their personal computing devices to conduct Mansfield University related business communications while operating a vehicle. This prohibition includes using a personal computing device to place or receive calls or voicemail messages, read or respond to e-mails, text messages, or instant

messages, surf the Internet, or for any other purpose related to Mansfield University business while operating a vehicle. Employees who are charged with traffic violations resulting from the use of their person computing device while driving will be solely responsible for all liabilities resulting from such actions.

I. DEVICES AND SUPPORT

All devices connected to the Mansfield University network are required to adhere to the Acceptable Use Policy. Devices must be registered under the users account and be current on all software updates and anti-virus solutions. Users are also required to follow the Policy on Digital Millennium Copyright Act (DMCA). CT may, without notification, prevent or ban any personally owned device which disrupts any University Computing resource or are used in a manner which violates any University policy.

Technical support for personally owned computing devices is limited to the following:

- Troubleshooting network connection issues while on the campus network.
- Troubleshooting and installation of approved University software resources.
- Configuration of the VPN client to allow access to secure resources with approval.
- Providing software application support if the software is required to perform job functions as determined by the Campus Technology department.

Examples of support services that will not be provided, but not limited to:

- Troubleshooting device performance or hardware problems
- Installation of new or replacement hardware
- Troubleshooting software applications or cloud services not offered or supported by Mansfield University
- Installing Operating System updates, patches or software applications not required for job functions
- Backing up device data or migration to another device
- Third party email clients/accounts
- Removal of malware, spyware or virus

II. USER RESPONSIBILITIES

As a user of Information Technology resources, employees have the following responsibilities:

- Responsible for all traffic originating from your networked devices whether you generate the traffic, or not.

- Responsible for abiding by all applicable laws set forth by Federal, State and Local Governments.
- Responsible for protecting your privacy.
- Responsible for not violating the privacy of others.
- Responsible for keeping your network devices up to date with current security patches.
- Responsible for using anti-virus software and ensuring that such software is at the most current release.
- Responsible for protecting any and all sensitive data for which you have access to.
- Responsible for following all applicable university policies relating to your use of Information Technology resources. These policies may be viewed at: https://www.mansfield.edu/policies-procedures/
- Responsible for ensuring the security of Information Technology resources under your direct control.
- Responsible for securing your granted access privileges and passwords for Information Technology resources.

III. RISK, LIABILITIES, AND DISCLAIMERS

Employees who elect to participate in BYOD accept the following risks, liabilities and disclaimers:

- At no time does the University accept liability for the maintenance, backup, or loss of data on a personal device; nor personal data. It is the responsibility of the equipment owner to backup all software and data to other appropriate backup storage systems before requesting assistance from Campus Technologies.
- At no time does the University accept liability for the security of the personal device when accessing the university networks.
- If determined that the use of the personal device is no longer required for job functions, the University may elect to discontinue providing computing resources to the device.
- The personally owned computing device is subject to the search and review as a result of litigation that involves the University.
- No employee should expect a guarantee of privacy in communications over the Internet and Mansfield University network.
- Violations of this Policy may be discovered by routine maintenance and monitoring of Mansfield University electronic communication systems and network, any method stated in this BYOD Policy, or pursuant to any legal means. The employee consents to Mansfield University monitoring, accessing, investigating, preserving, using and/or disclosing any electronic communications that utilize Mansfield University networks in any way, including data, voicemail, telephone logs, Internet use, network traffic, etc., to the extent permitted by law. Mansfield University reserves the right to review, retain or

release personal and Mansfield University-related data on personal computing device to government agencies or third parties during an investigation or litigation.

IV. REIMBURSEMENT

Computer technology purchased for personal use will not be reimbursed by the University. This includes all hardware, software, licenses, and technology services, including repair or technical support services purchased with personal funds, regardless of intended use.

V. ENFORCEMENT

Employees and other persons employed by the university found to have violated this policy will be subject to disciplinary action based on the nature of the offense up to and including termination of employment.

RESPONSIBILITY

It is the responsibility of the office of Campus Technologies to update and implement the policy, as needed.

DISTRIBUTION

This policy will be posted to the Policies and Procedures web page.