

**EASTERN WEST VIRGINIA COMMUNITY & TECHNICAL COLLEGE
BOARD OF GOVERNORS
POLICY NO. BP – 6.17**

TITLE: BRING YOUR OWN DEVICE (BYOD)

SECTION 1: GENERAL

- 1.1 Scope - This Bring Your Own Device (BYOD) policy outlines the guidelines and practices for students, faculty, and staff of the Eastern West Virginia Community and Technical College (“the college” or “Eastern”) who wish to use their personal electronic devices for educational and work-related purposes.
- This policy applies to all students, faculty, and staff who use their personal devices to access college resources, including but not limited to, email, course management systems, online learning resources, and college databases.
- 1.2 Authority – West Virginia Code 61-3C “West Virginia Computer Crime and Abuse Act”. WV Statewide Internet Acceptable Use Policy Guidelines
- 1.3 Effective Date - June 18, 2025
- 1.4 Applicability - This procedure applies to all students, faculty, staff, vendors and anyone with an account capable of connecting to the college network or access to college resources.

SECTION 2: DESCRIPTION

- 2.1 This policy applies to, but not limited to, the following mobile devices:
- Laptop/notebook/tablet computers.
 - Mobile/cellular phones.
 - Smartphones.
 - Home or personal computers used to access institutional resources; or
 - Any mobile device capable of storing corporate data and connecting to an unmanaged network.

Approved by IET (e-vote): 4/30/25

Approved by President’s Cabinet: 5/8/25

Posted for 30-day public comment period: 5/9/25 – No public comments received as of 6/10/25

Approved by the Board of Governors: 6/18/25

- 2.2 Compliance - All devices must adhere to this policy when connected to the network. Violation of this policy will result in disciplinary action.

SECTION 3: DEVICE RESPONSIBILITIES

- 3.1 Personal Devices - The use of personal computing devices to access college resources and data is on the rise among college students. A security breach occurring through such a device could lead to the loss or compromise of that said data. It could also cause damage or unauthorized access to college technology resources, potentially leading to financial implications for the college.
- 3.2 As a user of Information Technology resources, you have the following responsibilities:
- Users are responsible for all traffic originating from their networked devices whether you generate the traffic, or not.
 - Users are responsible for abiding by all applicable laws set forth by Federal, State and Local Governments.
 - Users are responsible for protecting their privacy. They are responsible for not violating the privacy of others.
 - Users are responsible for keeping their network devices up to date with current security patches.
 - Users are responsible for using anti-virus software and ensuring that such software is at the most current release.
 - Users are responsible for protecting any sensitive data to which they have access.
 - Users are responsible for following all applicable College policies relating to the use of Information Technology resources.
 - Users are responsible for ensuring the security of Information Technology resources under their direct control.
 - Users are responsible for securing their granted access privileges and passwords for Information Technology resources.

SECTION 4: PERSONAL USE

- 4.1 The following steps must be taken to ensure the security of all college information when utilizing mobile devices:
- 4.1.1. While at work, employees are expected to exercise the same discretion in using their personal devices as is expected for the use of college-owned equipment.

Approved by IET (e-vote): 4/30/25

Approved by President's Cabinet: 5/8/25

Posted for 30-day public comment period: 5/9/25 – No public comments received as of 6/10/25

Approved by the Board of Governors: 6/18/25

- 4.1.2. Review all college policies pertaining to harassment, discrimination, retaliation, trade secrets, confidential information, and ethics that apply to the use of personal devices for work-related activities.
- 4.1.3. Individuals who choose to use a personal device such as a smartphone, tablet, laptop, or notebook, to access Eastern Technology Resources are responsible for the following:
- Abiding by the requirements identified within this Policy.
 - Employees who have access to PII or sensitive data should never download or store it on a mobile device.
 - Any damages and criminal and/or civil charges resulting from the activities conducted on their personal device while connected to an Eastern server is the responsibility of the user.
- 4.1.4 **Password protection is key.** A strong password is defined as one that's difficult to detect by humans and computers, is at least 8 characters, preferably more, and uses a combination of upper- and lower-case letters, numbers and symbols. Some additional suggestions include:
- Do not use any words from the dictionary.
 - Avoid proper nouns or foreign words.
 - Do not use anything remotely related to your name, nickname, family members or pets.
 - Do not use any numbers someone could guess by looking at your mail like phone numbers and street numbers.
 - Choose a phrase that means something to you; take the first letters of each word and convert some into characters.
 - Use a feature that will lock your device automatically if it is idle for a set amount of time.

SECTION 5: STORAGE DEVICES

- 5.1 Current examples of portable storage devices include, but are not limited to, the following types of products:
- Magnetic storage devices (USB hard drives)
 - Optical storage devices (CDs, DVDs)
 - Memory storage devices (SD cards, thumb drives, etc.)
 - Portable devices that make nonvolatile storage available for user files (cameras, MP4 and music players, audio recorders, smart watches, cell phones).
- 5.2 There is no Eastern requirement to backup information, but it is highly recommended that device owners keep current and secured backups in case of device loss.

Approved by IET (e-vote): 4/30/25

Approved by President's Cabinet: 5/8/25

Posted for 30-day public comment period: 5/9/25 – No public comments received as of 6/10/25

Approved by the Board of Governors: 6/18/25

- 5.3 Notify Technology Services of any theft or loss of the personal device containing data belonging to Eastern immediately.
- 5.4 Restricted data in any format collected, developed, maintained or managed by or on behalf of Eastern, or within the scope of Eastern activities that are subject to specific protections under federal or state law or regulations or under applicable contracts are not to be stored on a personal storage device.

Examples include, but are not limited to, medical records, social security numbers, credit card numbers, driver license numbers, non-directory student records, research protocols, and export controlled technical data.

SECTION 6: SUPPORT FOR TECHNOLOGY

- 6.1 The only support services provided to personal mobile devices for troubleshooting network connection issues while on the campus network are configuration of email clients for connection to the email system and configuration of the SSL VPN client to allow access to secure resources with approval.
- 6.2 Support services that will not be provided, include, but are not limited to:
- Troubleshooting device performance or hardware problems.
 - Installation of new or replacement hardware
 - Troubleshooting software applications or cloud services provided by Eastern.
 - Installing operating system updates, patches or software applications not required for job functions is the responsibility of the user.
 - Backing up device data or migration to another device is the responsibility of the user.
 - Third party email clients/accounts are the responsibility of the user.
 - Removing malware, spyware or viruses is the responsibility of the user.

SECTION 7: RISKS/LIABILITIES/DISCLAIMERS

- 7.1 Those who elect to participate in BYOD accept the following risks, liabilities and disclaimers:
- 7.1.1 At no time does the College accept liability for the maintenance, backup, or loss of data on a personal device, nor personal data.
- 7.1.2. It is the responsibility of the equipment owner to backup all software and data to other appropriate backup storage systems.

SECTION 8: DEFINITIONS

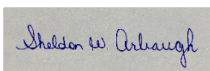
Approved by IET (e-vote): 4/30/25

Approved by President's Cabinet: 5/8/25

Posted for 30-day public comment period: 5/9/25 – No public comments received as of 6/10/25

Approved by the Board of Governors: 6/18/25

- 8.2 Loss - Devices used to transfer or transport work files could be lost or stolen.
- 8.3 Theft - Sensitive institutional data is deliberately stolen and sold.
- 8.4 Copyright - Software copied onto a mobile device could violate licensing.
- 8.5 Malware - Viruses, Trojans, Worms, Spyware and other threats could be introduced via mobile device.
- 8.6 Compliance - Loss or theft of financial and/or personal and confidential data could expose the college to the risk of non-compliance with various identity theft and privacy laws.



Board of Governors, Chair

06/23/2025

Date

Approved by IET (e-vote): 4/30/25

Approved by President's Cabinet: 5/8/25

Posted for 30-day public comment period: 5/9/25 – No public comments received as of 6/10/25

Approved by the Board of Governors: 6/18/25