PELLISSIPPI STATE COMMUNITY COLLEGE

POLICY 08:13:06
BRING YOUR OWN DEVICE (BYOD)

I. Purpose

The purpose of this policy is to define the appropriate use and procedures for using personally owned mobile and other devices on the college network and to protect the security and integrity of private and confidential institutional data residing in the college technical infrastructure.

II. Definitions

- **Mobile Device:** any device that can combine telecommunication and computing functions, or interact with such a device, and is easily carried on a person. Examples include, but are not limited to: laptop/notebook computers, smartphones (e.g. Apple iPhone, Android, Windows Mobile or RIM Blackberry, etc.), tablets (e.g. Apple iPad, Amazon Fire, Samsung Note, Microsoft Surface, etc.), personal digital assistants (PDA) or wearables (e.g. Apple Watch, Google Cardboard, HTC Vive, etc.)
- **Mobile Device Management (MDM)**: an application designed to manage mobile devices for an institution. MDM can provide delivery of patches and updates, delivery of college-purchased apps and security of devices by providing remote wiping of data if a device is lost or stolen.
- **Personal device**: any device that is not a college-owned.
- **Encryption:** using electronic or physical means to render clear text information unreadable to unauthorized persons.

III. Scope and Applicability

This policy applies to any employee, student, visitor, client or guest of the college who makes a connection from a personal device to any college provided network or connects to any college provided software, service, data or resource.

BYOD is a rapidly changing technology and Networking and Technical Services may elect to implement additional requirements or processes to safeguard the college's computing resources (e.g. mobile device management (MDM), remotely removing institutional data, or requiring additional registration processes).

IV. Risks, Liabilities, Disclaimers

To support the BYOD model while appropriately managing the college's risk, the following policies are established. Employees, students and guests who elect to participate in BYOD by making a connection from a personal device to any college provided network or to any college provided software, service, data or resource accept the following risks, liabilities and disclaimers:

- At no time does the college accept liability for the maintenance, backup, or loss of data on a personal device. It is the responsibility of the equipment owner to backup all software and data to other appropriate backup storage systems. The college also does not

accept liability for the security or loss of data for any visitor, client or guest of the college using a guest account or guest wireless network.

- The college shall NOT be liable for the loss, theft, or damage of any personal devices. This includes, but is not limited to, when the device is being used for college academic work or business activities, on college time, or during business travel.
- Information Services uses MDM on college-owned mobile devices. The college reserves the right to implement technology such as MDM to enable the removal of college owned data on personally owned devices if a reasonable security or privacy concern dictates that action.
- Persons violating this policy may also be held personally liable for resulting damages and civil or criminal charges. The college will comply with any applicable laws regarding data loss or breach notification and may also refer suspected violations of applicable laws to appropriate law enforcement agencies.
- A personal device that connects to any college provided network or connects to any college provided software, service, data or resource may be considered "discoverable."

V. User Responsibilities

Employees and students who elect to participate in BYOD must adhere to this policy and all college policies while using a personal mobile device on a college network or connecting to college owned services, resources, data or systems. In particular, all acceptable use provisions of Policy 08:13:01 Information Technology Acceptable Use are applicable.

A. Employees who elect to participate in BYOD accept the following responsibilities:

- Using reasonable physical security measures procedures such as enabling a PIN, password, biometric or other additional security features to prevent unauthorized access to the device and encrypting the device before connecting to college services, resources and/or data
- Refraining from storing sensitive work data or confidential student records and information as defined in Policy 04:03:00 - Student Records Confidentiality on a personal mobile device or unencrypted portable storage (e.g. USB thumb drive)
- Destroying, removing or returning all college owned data, electronic or otherwise, once your relationship with the college ends or once you are no longer the owner or primary user of the device. (e.g. the sale or transfer of a device to another person)
- Removing or returning all software application licenses belonging to the college when the personal device is no longer used for college business
- Notifying the HelpDesk of any theft or loss of a personal device containing data or software application licenses belonging to the college
- Not connecting a personal device to the wired college network without prior approval from the director of Networking and Technical Services. Before making a wired connection with a personally owned device, **the employee MUST contact the HelpDesk to start the approval process**
- Not connecting a personal mobile device that has been "jailbroken" or "rooted" to any college network, software, service, data, or resource. College owned mobile devices that are "rooted" or "jailbroken" MAY be allowed to join a college network with prior approval from the director of Networking and Technical Services
- Providing any necessary power cables and/or adapters required to connect to projection devices, audio reinforcement, sound systems or other guest connection hardware within

classrooms, auditoriums, meeting rooms and other college locations and comply with any posted instructions about connecting or disconnecting devices
- Following any announcements prohibiting live streaming or recording via personal devices of events, performances or other college activities.

B. Students of the college who elect to participate in BYOD accept the following responsibilities:

- Using reasonable physical security measures such as enabling a PIN, password, biometric or other security features to prevent unauthorized access to the device and encrypting the device before connecting to college services, resources and/or data
- Destroying, removing or returning all college owned data, electronic or otherwise, once your relationship with the college ends or once you are no longer the owner or primary user of the device. (e.g. the sale or transfer of a device to another person)
- Removing or returning all software application licenses belonging to the college when the personal device is no longer used for college work or business
- Not connecting a personal mobile device that has been "jailbroken" or "rooted" to any college network, software, service, data, or resource
- Notifying the HelpDesk of any theft or loss of a personal device containing data or software application licenses belonging to the college
- Not connecting a personal device to the wired college network without prior approval. **Before making a wired connection with a personally owned device, the student MUST contact the HelpDesk to start the approval process**
- Providing any necessary power cables and/or adapters required to connect to projection devices, audio reinforcement, sound systems or other guest connection hardware within classrooms, auditoriums, meeting rooms and other college locations and comply with any posted instructions about connecting or disconnecting devices
- Following any announcements prohibiting live streaming or recording via personal devices of events, performances or other college activities
- Understanding that a personal device may be used to record classroom activities as well as understanding that such recordings are the intellectual property of the faculty member or other person(s) being recorded and that the recordings are exclusively for personal learning purposes. Any recording required by a student's accommodation plan will always be permitted. Improper usage and distribution of recordings of classroom activities by students are considered violations of Policy 04:02:00 Student Code of Conduct and Due Process.

C. Visitors, guests and clients of the college who elect to participate in BYOD accept the following responsibilities.

- Using reasonable physical security measures such as enabling a PIN, password, biometric or other security features to prevent unauthorized access to the device and encrypting the device before connecting to college services, resources and/or data
- Destroying, removing or returning all college owned data, electronic or otherwise, once your relationship with the college ends or once you are no longer the owner or primary user of the device. (e.g. the sale or transfer of a device to another person)
- Removing or returning all software application licenses belonging to the college when the personal device is no longer used for college work or business
- Not connecting a personal mobile device that has been "jailbroken" or "rooted" to any college network, software, service, data, or resource

- Notifying the HelpDesk of any theft or loss of a personal device containing data or software application licenses belonging to the college
- Not connecting a personal device to the wired college network without prior approval. **Before making a wired connection with a personally owned device, the owner MUST contact the HelpDesk to start the approval process**
- Providing any necessary power cables and/or adapters required to connect to projection devices, audio reinforcement, sound systems or other guest connection hardware within classrooms, auditoriums, meeting rooms and other college locations and comply with any posted instructions about connecting or disconnecting devices
- Following any announcements prohibiting live streaming or recording via personal devices of events, performances or other college activities.

VI. Devices and Support

In general, any computing or mobile device may be connected to any college wireless network provided its use does not disrupt any college computing resources or violate Policy 08:13:01 Information Technology Acceptable Use. Personal mobile devices are expected to be kept current with security updates provided by the device and operating system vendors.

Information Services will prioritize the support of PSCC owned computing devices and production systems and provide only limited support for personal devices as defined in the Networking and Technical Services procedures manual.

VII. Privacy

The college will always respect the privacy of a personal mobile device and will only request access to the device by technicians to implement security controls or to respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings.

VIII. Security

College-owned mobile devices are managed and distributed by Information Services as stated in the Policy 08:13:01 Information Technology Acceptable Use. Information Services staff will maintain administrative control of such devices including remote lock and remote wipe functions which might be used in the event of loss or theft of the device. NTS will also maintain and enforce encryption of the internal storage of the device.

However, NTS reserves the right to implement such restrictions or solutions on a personal device or devices based on emerging and/or urgent security or privacy concerns. NTS may perform security scans against any personally-owned device that accesses college networks, services, resources, data or applications in accordance to Policy 08:13:01 Information Technology Acceptable Use and TBR Policy G-052 - Access Control. NTS may, without notification, prevent or ban any personal mobile device which disrupts any college computing resources or is used in a manner which violates any college policy.

IX. Enforcement

Suspected violations of this policy will be handled through the college disciplinary procedures applicable to the relevant user in accordance with Policy 08:13:01 Information Technology Acceptable Use. NTS may suspend a user's access to the college network and/or any data, service, resource or software prior to the initiation or completion of such disciplinary procedures, when it reasonably appears necessary to preserve the integrity, security, or functionality of college data and services or to protect the college from liability. The college may also refer suspected violations of applicable laws to appropriate law enforcement agencies.

The Director of Networking and Technical Services shall be the primary contact for the interpretation, enforcement and monitoring of this policy and the resolution of problems concerning it. Any legal issues concerning the policy shall be referred to the appropriate officials for advice.

Reviewed/Recommended: President's Council, November 20, 2017
Approved: President L. Anthony Wise, Jr., November 20, 2017
Editorial Changes November 26, 2019