**
University of Northern Colorado**

**Campus Administration Policy for Personal Devices (Bring Your Own Device - BYOD) when Working Remotely or In-Office**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**A. INTRODUCTION**

The University of Northern Colorado (UNC) recognizes that university employees, and Graduate students, at times utilize their Personal Devices when conducting University business. In response to an increase in Personal Devices being used in the work environment and remotely, UNC has established an official Bring Your Own Device (BYOD) policy. Nothing in this policy requires a department or UNC to compensate those who utilize their own Personal Devices. BYOD is the act of using Personal Devices for University work or business-related activities. Employees who use their Personal Devices for University work- or business-related activities must abide by the policy below.

**B. DEFINITIONS**

1. **Data Encryption** means securing data into another form, or code, so that only people with access to a secret key (formally called a decryption key) or password can read it.

2. **Personal Device** means cellular smartphones, tablets, laptop or desktop computers or any employee-or student-owned device utilized for UNC related communications or accessing data or confidential information.

3. **Personally Identifiable Information** means 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, initials, Bear Number, 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.

4. **Sensitive Information** means any information that can be used to identify a person. Examples include personal information, medical records, financial information, UNC administrative computer data (employee records, student records, electronic documents that contain confidential information), passwords and account details, and research data. This includes information protected by The Family Educational Rights and Privacy Act (FERPA) and Health Insurance Portability and Accountability Act (HIPAA).

**C. POLICY STATEMENT**

1. **Purpose**

The purpose of this policy is to outline the responsibilities and obligations of UNC employees and graduate students who participate in the BYOD program. This policy defines the acceptable use and procedures for using Personal Devices, the storage and transmission of sensitive data, confidential and highly confidential data, and an employee’s and student’s obligation to maintain UNC related communications on a secure system.

**D. GENERAL RULES**

Users shall comply with federal and state laws, University rules, regulations, and policies.

Users must follow the University records retention policy and any records retention policy that might apply.

Users shall protect and secure Private Health Information (PHI).

Users are responsible for any activity originating from their accounts which they are expected to control.

If unauthorized use of accounts is detected or suspected, the account owner should change the password and immediately report the incident to UNC IT and the Department Director, or Chair.

Users must understand that disclosing their account credentials to cybercriminals may result in personal losses for which they are responsible.

**E. POLICY STATEMENT**

1. **Account Use**

a. Users shall utilize their accounts only for the purposes specified by the account grantor.

b. Users shall not use any other individual's credentials or attempt to access an account when authorization has not been granted for them.

c. Users shall not attempt to alter or avoid account access controls for computing systems.

d. Accounts and passwords may not, under any circumstances, be used by persons other than those to whom the account administrator has assigned them.

e. Users shall not share/disclose their account passwords with others.

f. Users shall install and enable encryption, firewall, and security software.

**2. Privacy**

a. Users shall not intentionally seek information on, obtain copies of, or modify files, hard drives, passwords or credentials, or any type of data belonging to other users.

b. Users should always avoid violating privacy by:

i. Tampering with security provisions.

ii. Attempting entry to non-public hosts.

iii. Sharing login credentials with others.

**3. Computer and Network Security**

a. Users shall not attempt to alter, delete, or avoid computer audit controls and accounting log files.

b. Users shall not attempt to bypass computer and network controls.

c. Users should not send unencrypted information on Personal Devices

d. Do not ignore security software updates.

e. Do not leave Personal Devices unattended.

f. Always use a secure Wi-Fi network.

g. Do not discard Personal devices without deleting stored information and wiping device.

**4. Legal and Ethical Use**

Users shall not:

a. Abuse, harass, intimidate, threaten, stalk, or discriminate against others using computing resources.

b. Send obscene, abusive, harassing, or threatening messages to any other individual.

c. Misrepresent oneself or others through electronic communication, including email.

d. Engage in physical or cyber vandalism or mischief that incapacitates, compromises, or destroys UNC IT resources.

e. Download or save obscene, pornographic, or otherwise offensive documents, images, videos, or other files onto their work computer.

f. Post any work-business-related personal information on any social media platform.

**F. RESPONSIBILITY AND ACTION**

Violation of this policy or other University information technology policies can result in revocation of computing privileges as well as corrective and/or disciplinary action.

Other offices, departments, schools, etc. may be responsible for campus compliance and enforcement of this policy to take further action against violations.

Users who violate this policy may be subject to other penalties and disciplinary action, including expulsion or dismissal. Other responsible parties may also refer suspected violations of the law to appropriate law enforcement agencies for further investigation or action.

The University may suspend, block, or restrict access to an account when it appears necessary:

a. to protect the integrity of UNC security resources.

b. to comply with legal or contractual requirements.

c. to investigate alleged or potential violations of law or policy including, without limitation, state, federal, or local law, UNC rules, regulations, policies, or collective bargaining agreements.

d. to investigate any potential complaint or grievance, or subject of law enforcement review or investigation. pursuant to rules, regulations, policies, and law.

e. or to protect the University from liability or disruption.

**2. Responsibility**

The University is not responsible for the purchase or costs associated with use of employee-owned Personal Devices. The University is not responsible for technical support or repair of employee-owned Personal Devices. The employee is responsible for providing the device and complying with this policy.

**3. Expectations and Acknowledgements**

Employees who participate in the BYOD policy must:

a. Not store any University communication, University data or University intellectual property exclusively on Personal Devices.

b. Appropriately secure and encrypt the device and delete data before disposing of device.

c. Notify their department and the University of any theft or loss.

d. Notify their department and the University of any change in telephone number, if applicable.

e. Comply with local laws while operating a motor vehicle if conducting University business via cell phone.

f. Abide by all applicable laws set forth by Federal, State and Local Governments.

**Employees and Graduate Students acknowledge that:**

a. All communications related to University business are public records as defined by the Colorado Open Records Act (CORA), Title 24, Article 72. Patient records, including Secure Chat are not a public record under CORA, but are still subject to other legal action such as subpoena or court order.

b. As a condition of using a Personal Device to perform University business any and all University related communication, data and work performed on a Personal Device will be stored on a secure system that can be accessed as necessary by the University to perform business including, but not limited to responding to open records requests or other official requests, including a subpoena and any personnel related investigations related to employee’s performance.

• If an official request is made, text (SMS) messages must be electronically extracted and submitted to the requesting entity.

c. If using Personal Devices for transmitting or communicating patient information, Personally Identifiable Information, or Sensitive Information, employee/student agrees to use Data Encryption applications to protect this information.

**4. Sanctions**

Violation of this policy or other university information technology policy can result in corrective and/or disciplinary action under applicable University rules, regulations, and policies. Sanctions for HIPAA violations can result in fines ranging from $100 to $250,000 (with a $1.5 million annual ceiling) as well as prison terms of 1 to 10 years.

**By signing this statement, I agree to follow UNC’s policy and procedures for BYOD and when using a Personal Device.**

**Print name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_­**

 **Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

 **Bear Number: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Department: ­­­­­­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

 **Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**