| | | |
|---|---|---|
| Prescott College | **Policy Number:** *1225* | |
| | **Policy Category:** *Information Technology Policies* | |
| | ***Mobile Device Acceptable Use*** | |
| | **Policy Summary:**<br><br>*This policy defines standards, procedures, and restrictions for any and all end users with legitimate business uses connecting mobile devices to Prescott College's corporate network, digital resources, and data.* | |
| | **Approval Date:**<br>*04-22-24* | **Effective Date:**<br>*Upon approval* |
| **Policy Owner:**<br><br>*Vice President, Finance and Administration* | **Scheduled for Review:**<br><br>Spring 2029 | |

## Policy Statement

Prescott College employees using a mobile device to access corporate resources have the responsibility to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. Any mobile device that is used to conduct Prescott College business must be used appropriately, responsibly, and ethically. Failure to comply with this policy will result in immediate suspension of that user's account.

Based on this requirement, the following rules must be observed:

1. Access Control
    a. End users who wish to connect such devices to non-corporate network infrastructure to gain access to enterprise data must employ, for their devices and related infrastructure, security measures deemed necessary by the IT department. Enterprise data is not to be accessed on any hardware that fails to meet Prescott College's established enterprise IT security standards.
    b. All personal mobile devices attempting to connect to the corporate network through the Internet will be inspected by Prescott College's IT department. Devices that are not approved by IT, are not in compliance with IT's security policies, or represent any threat to the corporate network or data will not be allowed to connect.
    c. IT reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to corporate and corporate-connected infrastructure. IT will engage in such action if such equipment is being used in a way that puts the company's systems, data, users, and clients at risk.

2. Security
    a. Employees using mobile devices and related software for network and data access will, without exception, use secure data management procedures. All mobile devices must be protected by a strong password; a PIN is not sufficient. See Prescott College's password policy at https://prescott.edu/policies-and-resources/ for additional background. Employees agree never to disclose their passwords to anyone.

b. All users of mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices against being lost or stolen, whether or not they are actually in use and/or being carried.
c. Any non-corporate computers used to synchronize or backup data on mobile devices will have installed up-to-date anti-virus and anti-malware software deemed necessary by Prescott College's IT department.
d. Passwords and other confidential data, as defined by Prescott College's IT department, are not to be stored unencrypted on mobile devices.
e. Any mobile device that is being used to store or access Prescott College data must adhere to the authentication requirements of Prescott College's IT department. In addition, all hardware security configurations must be pre-approved by Prescott College's IT department before any enterprise data-carrying device can be connected to the corporate network.
f. The IT department will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass that security implementation will be deemed an intrusion attempt and will be dealt with in accordance with Prescott College's overarching security policy.
g. Employees, contractors, and temporary staff accessing Prescott College internet resources from a smartphone or tablet will NOT save their user credentials or internet sessions when logging in or accessing company resources of any kind.
h. Employees, contractors, and temporary staff will follow all enterprise-sanctioned data removal procedures to permanently erase company-specific data from such devices once its use is no longer required.
i. In the event of a lost or stolen mobile device, the user is required to report the incident to IT immediately.

3. Hardware& Support
   a. IT reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the enterprise network.
   b. Users will make no modifications to the hardware or software that change the nature of the device in a significant way (e.g. replacing or overriding the operating system, jail-breaking, rooting) without the express approval of Prescott College's IT department.
   c. IT will support the connection of mobile devices to corporate resources. On personally owned devices, IT will not support hardware issues or non-corporate applications. See https://tech.prescott.edu for full help desk and tech support policies.

4. Organizational Protocol
   a. IT can and will establish audit trails, which will be accessed, published, and used without notice. Such trails will be able to track the attachment of an external device to the corporate network, and the resulting reports may be used for investigation of possible breaches and/or misuse. The end user agrees to and accepts that his or her access and/or connection to Prescott College's networks may be monitored to record dates, times, duration of access, etc. in order to identify unusual usage patterns or other suspicious activity. The status of the device, including location, IP address, Serial Number, IMEI, may also be monitored. This monitoring is necessary in order to identify accounts/computers that may have been compromised by external parties or users who are not complying with Prescott College's policies.

b. The end user agrees to immediately report to his/her manager and Prescott College's IT department any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of company resources, databases, networks, etc.
c. Prescott College will not reimburse employees if they choose to purchase their own mobile devices. Users will not be allowed to expense mobile network usage costs.
d. Any questions relating to this policy should be directed to the IT Helpdesk, at 928-350-4400 or helpdesk@prescott.edu.

Devices covered under this policy include, but are not limited to the following classifications:

- Smartphones
- Other mobile/cellular phones
- Tablets
- E-readers
- Portable media devices
- Portable gaming devices
- Laptop/notebook/ultrabook computers
- Wearable computing devices
- Any other mobile device capable of storing corporate data and connecting to a network

Failure to comply with this policy may result in the suspension of any or all technology use and connectivity privileges, disciplinary actions and possibly termination of employment.

**Definitions**

**Reason for Policy**

To protect the integrity of the confidential client and business data that resides within Prescott College's technology infrastructure, including internal and external cloud services.

| **Responsibilities** | |
|---|---|
| For following policy: | All persons using a mobile device to access, store, backup or relocate any enterprise data. |
| For enforcement of policy: | Director, Information Technology |
| For oversight of policy: | Director, Information Technology |
| For procedures implementing the policy: | Director, Information Technology |
| For notification: | Policy Librarian |

**Procedures**

**Cross Referenced Policies**

**Revision History**