

## Mobile Device Policy

### Purpose

The purpose of this policy is to define standards, procedures, and restrictions for end users who may have a legitimate business need to access Clayton State University's (CLSU) sensitive and confidential information, or non-public university information from a mobile device. This mobile device policy applies to, but is not limited to, all devices and accompanying media that meet the following device classifications:

- Handheld computers or tablets.
- Laptops.
- Smartphones.
- USB Flash drives or portable hard drives
- Home or personal computers used to access campus resources.
- Any other mobile device capable of storing campus data and connecting to an unsecured network.

The intent of this policy is to protect the university's confidential/sensitive information from being deliberately or inadvertently breached or stored on an unsecured device, unapproved cloud storage, or unsecured network. A breach of this type could result in loss of confidential/sensitive information, damage to critical applications, loss of revenue, and damage to the institutions' public image. Therefore, all users employing a mobile device connected to the campus network or off-campus unmanaged network to backup, store, and otherwise access campus information of any type must adhere to CLSU defined policies, standards, and processes.

### Applicability

This policy applies to all CLSU employees, including full- and part-time staff, consultants and other agents who use a university or personally owned device to access, store, backup or relocate any CLSU or client-specific data. Such access to these data is a privilege, not a right, and forms the basis of a trust CLSU has built with its clients, vendor partners and other constituents. Consequently, CLSU employment does not automatically guarantee the initial or ongoing ability to use personal devices to gain access to university networks and information.

This policy applies to any hardware and related software that is or is not owned or supplied by CLSU but could be used to access campus resources. This includes devices that employees have acquired for personal use, or a legitimate business need. It includes any portable device capable of inputting, processing, storing, and outputting CLSU data. This policy is complementary to any previously implemented policies and standards covering acceptable use, data access, data storage, data movement and processing, and connectivity of devices to any element of the institution's network.

### Policy and Appropriate Use

It is the responsibility of all CLSU employees, including full- and part-time staff, consultants and other agents who use a mobile device to access university resources to ensure all security

protocols used in the management of confidential, sensitive, or non-public information on the institution's information systems is applied. Any mobile device used to conduct Clayton State University business be utilized appropriately, responsibly, and ethically.

## Personal Mobile Device Policy

*(Formerly known as BYOD)*

Although CLSU ITS service providers are charged with preserving the integrity, confidentiality, availability, and security of CLSU managed data and information resources, security may be compromised through actions beyond any user's control. Among these, personally owned mobile devices or so-called bring-your-own-devices (BYODs) used by any user presents a special risk to CLSU resources because device owners install and configure software applications, security settings and perform their own maintenance and may share the device with others. A CLSU employee may use a personal mobile device to access CLSU resources only if the employee receives permission from their direct supervisor AND permission from the Data Steward responsible for the resources the employee needs to access.

Note: Use of personal device for authentication purpose only to CLSU resources is **NOT** required to register their device with the university.

### Application for Permission to Use Personal Mobile Device

A CLSU employee may request permission from their supervisor and the appropriate Data Stewards by completing the *Personal Mobile Device Authorization form*. The form must be completed by the employee with the following information

- 1) **CLSU Supervisor**
  - a. Determining the types of devices and software versions that are permitted;
  - b. Detailing which non-CLSU BYOD applications are supported;
  - c. Disclosing the type of action taken on personal mobile devices when employees are terminated or separated;
  - d. Providing a disclaimer of liability for personal data loss; and
- 2) **CLSU Data Steward:**
  - a. Describing what organizational information is permitted on personal devices;
  - b. Notifying users of disclosure requirements under the Georgia Open Records Act.
- 3) **CLSU Information Security**
  - a. Defining the minimum level of access controls, which may include device registration, VPN connection, and anti-virus protection;
  - b. Detailing the types of data protection and security required for permitted devices;
- 4) **The user/owner of the personal mobile device, shall:**
  - a. Safeguard CLSU account credentials and use multi-factor authentication where possible;
  - b. Use a Virtual Private Network (VPN) connection, personal firewall and antivirus protection;

- c. Back up CLSU data regularly and store all CLSU data in CLSU-managed infrastructure employing CLSU One Drive;
- d. Avoid the use of unauthorized third-party software or storage facilities for CLSU information;
- e. Install security patches in a timely manner;
- f. Promptly report CLSU data loss from personal mobile devices, misuse, or violation of this standard; and
- g. Comply with applicable policies and laws when using personally owned devices.

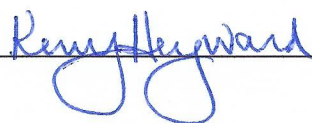
References & Supporting Documents

- [CLSU Security Policies](#)
- [CLSU Policies and Procedures](#)
- [USG IT Handbook & resources](#)

Approvals

Print: James A. Pete Signed  Date: 9/21/2022

CIO

Print: Kerry Heyward Signed  Date: 9/22/22  
President