Status **Draft** PolicyStat ID **21285708**

UNIVERSITY OF WEST GEORGIA

Last Approved	N/A
Effective	N/A
Next Review	N/A
Area	IT/ Management (Procedures)
Responsible Party	Information Technology Services

Bring Your Own Device

Authority for Procedure granted by UWG Policy #5002, Data Security.

This procedure establishes the standards for the University of West Georgia's (UWG) Bring Your Own Device (BYOD) program, outlining the requirements for using personal Computing Devices to access University Information Technology (IT) Resources.

It applies to all Users who use personal devices to access University IT Resources or University Owned Data. Contractors acting on behalf of the University of West Georgia must follow the access requirements outlined in their contracts and may also be subject to this procedure.

Authorized Users are permitted to access University of West Georgia IT Resources and University-Owned Data using personal devices, provided they comply with the University's Acceptable Use *(UWG PL 5001, Acceptable Use for Computers and Network*) and these BYOD procedures. Such access is granted at the University's discretion and is contingent upon the user adhering to all applicable policies and procedures.

By accessing the University System of Georgia (USG) or UWG IT Resources, users acknowledge, consent to, and agree to comply with all University policies governing access, security, monitoring, and Data management. The University reserves the right to monitor activity to detect, prevent, and respond to unauthorized access or potential security threats, including compromised accounts or devices.

A. BYOD Privacy Expectations

No person using their personal device should expect any privacy except that which is governed by law. The University of West Georgia has the right to monitor the use of and preserve any communications that use University IT Resources in any way, including but not limited to Data, voice mail, telephone logs, Internet use, and network traffic, for compliance and to determine appropriate use.

Authorized Users are **not** allowed to use a personal device to access IT Resources when prohibited by policy, regulation, or law.

Authorized Users who use personal devices for University business acknowledge that, despite personal ownership of the device, all University policies governing IT Resources remain in effect. The University reserves the right to revoke access to IT Resources and remove University-installed software from personal devices at any time if deemed in the University's best interest. Additionally, any alternative security measures not explicitly outlined in these procedures must be approved by the University Chief Information Officer (CIO) and are subject to the discretion of the USG Chief Information Security Officer (CISO).

Employees must provide any University-Owned Data that is Stored on personal devices if required for legal or regulatory purposes, such as requests under the Georgia Open Records Act, the Family Educational Rights and Privacy Act (FERPA), or legal orders (e.g., warrants, subpoenas, court orders). Any access or review of personal devices will be limited to the scope necessary to comply with the specific request or legal requirement.

B. Mobile Application Management (MAM)

The University reserves the right to implement technology to enable the access, review, and removal of University-Owned Data from personal devices.

Many faculty and staff use personal devices to access university email, Teams, OneDrive, and other Microsoft 365 applications. We also understand that protecting your personal privacy is just as important as protecting university data.

UWG utilizes mobile application management (MAM) to secure University Owned Data within supported Microsoft apps by encrypting information, enforcing security policies, and preventing accidental sharing of university data, all without accessing your personal photos, text messages, personal emails, contacts, passwords, browsing history, or other personal information. In most BYOD scenarios, device enrollment is not required.

If a device is lost or an employee leaves the university, ITS can remove only University Owned Data from protected apps while leaving your personal content completely untouched.

C. BYOD Requirements

Employees must comply with the following device requirements when accessing University IT Resources from personal devices:

Primary Use Restriction: Personal devices shall not be used as the primary means to create, store, send, or receive University Owned Data.

Access to Sensitive Data: Employees who need to access Sensitive Data must use a University-issued device unless one is unavailable. In such cases, an Employee is allowed to use a personal device only when accessing Data through an approved University remote access solution.

Security and Configuration Compliance: Authorized Users are expected to protect personal devices

used for work-related purposes from loss, damage, and theft. Personal devices must meet the University's minimum security standards for personal device configuration and maintenance, including:

- Unique password/pin protection (e.g., complex password, multi-factor authentication, encryption, biometric authentication, etc.) of the device.
- Locking the device when not in use.
- Prohibiting the sharing of passwords, passcodes, or other authentication credentials.
- Employees are **not** allowed to install or make modifications to personally owned hardware or software that circumvent established security protocols.

In keeping with best practices for BYOD devices, it is recommended that all devices utilize encryption and maintain a functioning and up-to-date anti-virus solution. Devices should be patched to appropriate and supported OS versions.

Technical Support Limitations: University IT support personnel are **not** responsible for installing, troubleshooting, or upgrading personal devices, except when related to University-managed applications and services.

Software Restrictions: Employees are not allowed to download University-licensed software onto personal devices unless specifically permitted by the software license (e.g., Microsoft Office).

Data Handling:

- Employees are **not** allowed to download or store Confidential Data (i.e., restricted) to a personal device.
- Any Sensitive Data or Personally Identifiable Information (PII) inadvertently Stored on a personal device must be deleted immediately.
- Sensitive, Personally Identifiable Information, Confidential Data must be protected using Data encryption while in transit.
- Employees must follow the University's Records Information Management Policy regarding the retention and disposal of University records on personal devices.
- Employees must appropriately dispose of University-Owned Data downloaded to a personal device when:
    - Their employment with the University ends.
    - They no longer require access due to a change in job responsibilities.
    - They are no longer the owner or primary user of the device.

Timekeeping compliance for Nonexempt Employees: Nonexempt Employees may **not** access University IT Resources outside of working hours without express written permission from their supervisors.

Lost, stolen, hacked, or damaged equipment requirements

The University of West Georgia is **not** liable for the loss or damage of personal devices, applications, or Data resulting from the use of University IT applications.

If a personal device used to store University-Owned Data or access University IT Resources is **Lost, stolen, or hacked**, Employees are required to notify ITS immediately via the ITS Support Portal. *Upon receiving the report, the ITS Chief Information Security Officer (CISO) will attempt to disable access to University applications, and all University-related Data on the device may be remotely wiped or erased.*

Employees must immediately notify Information Technology Services (ITS) of any actual or suspected incidents involving unauthorized Data access, Data loss, or disclosure of University system or participant organization resources related to personally owned devices.

D. Recourse for Noncompliance

Employees using personal devices to access University IT Resources acknowledge and agree that the University may access these devices as necessary to fulfill its obligations regarding the use and disclosure of University-Owned Data.

To ensure compliance with this procedure, the University reserves the right to audit any personal device used to access University IT Resources. Any instances of non-compliance must be reviewed and approved by the Chief Information Officer (CIO), Chief Information Security Officer (CISO), or equivalent officer(s), in consultation with the University General Counsel.

All actual or suspected Information security breaches must be reported to and investigated by the CISO. Individuals who violate security policies, standards, or procedures may face disciplinary action, including revocation of access to University IT Resources and other appropriate measures as determined by the University.

Additionally, violations may also breach other University policies and laws, subjecting individuals to civil and/or criminal prosecution.

Definitions

Authorized User - An individual who has been granted permission by the University of West Georgia (UWG) to access University IT Resources and University-Owned Data. Authorized Users may include, but are not limited to, faculty, staff, students, contractors, vendors, and other affiliated individuals. Access is granted based on role-specific requirements and is contingent upon compliance with University policies, procedures, and applicable legal and regulatory requirements.

Computing Device - General term that includes computer desktops, laptops, tablets, smartphones, and other specialized IT equipment.

Confidential - Information maintained by the institution that is exempt from disclosure under the provisions of the Open Records Act or other applicable state or federal laws. This includes information

whose improper use or disclosure could adversely affect the ability of the institution to accomplish its mission, records about individuals requesting protection under the Family Educational Rights and Privacy Act of 1974 (FERPA), or data not releasable under the Georgia Open Records Act or the Georgia Open Meetings Act.

Data - Individual facts, statistics, or source information stored for reference or analysis.

Employee - Any person in a non-student position at the University of West Georgia who receives compensation from the University and where the University has the right to control and direct how the work is performed.

Information - Data that is processed, organized, and structured. It provides context for the Data and enables decision-making.

IT Resources - Includes Computer Networks, Computing Devices, and Information Systems used to store, process, or transmit Information and/ or Data, and additionally includes all such Information and Data.

Nonexempt Employee - An employee covered by (not exempt from) the protections of the Fair Labor Standards Act (FLSA). A nonexempt employee is subject to the FLSA's minimum wage, overtime, and record-keeping requirements.

Sensitive - Data for which users must obtain specific authorization to access since the data's unauthorized disclosure, alteration, or destruction will cause potential damage to the participant organization. Example: Personally Identifiable Information, Family Educational Rights and Privacy Act {FERPA), Health Insurance Portability and Accountability Act {HIPPA) data, or data exempt from the Georgia Open Records Act.

Sensitive Personally Identifiable Information (Sensitive PII) - personally identifiable information that if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual, such as a Social Security number or alien number (A-number). Sensitive PII requires stricter handling guidelines because of the increased risk to the individual if compromised.

Stored - Data held or at rest, either locally or in the cloud.

University-Owned Data – Any data created, collected, received, processed, stored, transmitted, or maintained by the University, or on the University's behalf, in the ordinary course of conducting University business, academic programs, research, administration, or operations. This includes data created or managed by employees within the scope of their employment or official University responsibilities, regardless of whether the data is stored on University-owned systems, personal devices, cloud services, or third-party platforms.

University-owned data also includes data created or maintained by student employees, interns,

contractors, consultants, volunteers, or other individuals acting on behalf of the University(this definition generally does not include data created by students solely as part of their individual academic activities). Students engaged in research that utilized University data should refer to and adhere to IRB requirements.

Employees and other authorized individuals serve as custodians of such data and do not acquire personal ownership of it by creating, accessing, modifying, or maintaining it.

Approval Signatures

Step Description	Approver	Date
	Tara Pearson	08/2021