WGTC 1.13

Mobile Devices

West Georgia Technical College provides mobile devices to employees to support the effective performance of their jobs. They are intended for business purposes only. Each individual who receives a mobile device is responsible for safeguarding the equipment and controlling its use.

Guidelines:
The employee assigned the use of a cellular device is expected to exercise discretion regarding persons having access to the employee's cellular phone number in an effort to minimize phone usage costs while maintaining department service capabilities.

Cellular phones, mobile devices, and hotspots are not to be used when a less costly alternative is readily available.

Employees using an issued cellular phone are not permitted to withhold their cellular phone number from other employees who need it to conduct business.

The college will provide one (1) data enabled device to users that have multiple mobile devices. Exceptions are on a case-by-case basis, with executive approval required.

Eligibility:
Employee eligibility under this guideline will be defined as employees at the executive level or:

- Employees whose primary job duties are performed outside of an office environment
- Employees required to be accessible 24 hours a day, 7 days per week for emergencies
- Employees who must work at multiple locations
- Other critical contacts (public safety, IT staff, and key facilities staff)

Data Security:
Any mobile device used for business communications must be password, pattern, or PIN protected at all times when not in use. The device must be configured so that if the password, pattern, or PIN is incorrectly entered ten times, the device must reset to factory defaults (all data erased).

Employees must understand that any device (personal or College issued) used for business communications is subject to remote wipe of all contents by the College Information Security Administrator (ISA), if deemed a security issue. Employees are responsible for securing their

devices to prevent non-public data from being lost or compromised. Information not intended for public dissemination should never be transmitted.

Usage:
The use of College owned cellular equipment for personal use is strongly discouraged, although it is understood that usage for personal reasons may be necessary in emergency situations when no other immediate means of communication are available to the employee.

Employees must realize that, although personal calls are under the usage limits provided by the employee's plan, they do count toward the overall time limits established under the College's service agreement.

Employees are responsible for promptly reimbursing the College for all non-business cellular device charges incurred. This practice shall apply to both incoming and outgoing cellular phone calls.

It is also recognized that these devices are connected to the Internet and College networks. Please refer to the Computer Use and Internet Use guidelines for guidance on acceptable usage.

The College also acknowledges that some mobile devices are capable of making online purchases from retailers. The College will not reimburse the cost of these purchases, and if purchases are applied to the monthly invoice, the employee will reimburse the College.

Employees who have been issued multiple mobile devices will have only one device "data enabled" paid for by the College.

Employees are not permitted to operate a personal business from a College-issued mobile device.

Damage, Loss, or Theft:
Employees should take reasonable precautions to prevent loss, damage, theft, or vandalism to College-issued mobile devices.

The College will accept responsibility for equipment that is damaged in the course of business unless the damage is the result of reckless or deliberately destructive actions of the employee.

Equipment that is lost, stolen, or damaged outside the course of business is the responsibility of the employees to which the device is assigned. The Information Technology Department will have pricing information for the cost of a replacement device.

All damaged equipment should be brought to the attention of the employee's supervisor and the College Information Security Officer (ISO). The supervisor or employee will contact the Information Technology Department, who will contact the vendor for replacement or repair. Employees and supervisors are NOT to contact the cellular provider directly.

All lost or stolen equipment should be reported to the ISO immediately so the service can be suspended or cancelled and the device can be remote wiped of contents.

Safe Use:
In the interest of safety, employees using mobile devices are expected to exercise appropriate care and caution if used in a moving motor vehicle. Employees are to avoid the use of mobile equipment under any circumstances where such use might create or appear to create a hazard. Employees should use mobile devices only when the vehicle is not in operation.

It is recommended to utilize hands-free technology. If the vehicle is equipped with hands-free technology, or if you own a hands-free headset, that can be utilized. The College does not provide hands-free technology and, therefore, discourages the use of cellular devices while driving.

Personal Devices:
West Georgia Technical College will not reimburse employees for business calls or Internet usage made on non-College devices. Employees who feel they need to use a cellular phone or have mobile Internet service for College business must follow the guidelines to acquire a College-issued device.

Personal mobile devices can be utilized if the employee is wiling to fund and support the device. If the device is configured to use the College network or retrieve employee email, the employee acknowledges that College guidelines require that any computer/device connected to the network is subject to the "State of Georgia Open Records Act." (This means that during a security audit, a list of remote users could be requested, and if deemed that those users connected to State resources from non-state devices, the equipment could be susceptible to search and/or seizure.)

College email, data, and other business-related communications are the property of the College regardless of where they are stored; the mobile devices used for business communications are subject to search and/or seizure at any time; and there is no guarantee or expectation of privacy for any communications or data (personal or otherwise) stored on the device used for business communications.

Lost personal devices or stolen equipment should be reported to the ISO immediately so the email services can be suspended and the device can be remote wiped of contents, if necessary.

Usage Monitoring:
Cellular invoices will be audited on a monthly basis (or other such periods as the College may direct to examine usage). The College has the right to terminate and/or suspend or alter plans at any time. Employees will be made aware of overages or other incurred charges outside of normal billing.

Normal billing includes:

- Allocated talk time minutes
- Limited data plan (depends on device) and, in some instances, unlimited data
- Mobile to mobile unlimited talk time (AT&T to AT&T or Verizon to Verizon)
- Text messaging services

Penalties:
Violations of these policies incur the same types of disciplinary measures as violations of other WGTC policies or state or federal laws, including criminal prosecution.

Policy Source: West Georgia Technical College	Policy Manager: Executive Director, Information Technology	Effective: 9/2021
Division: Information Technology	Reviewed: Revised:	