Policy on the Deployment and Use of University-Owned Mobile Devices

Title:	Deployment and Use of University-Owned Mobile Devices
Policy number:	POL 010
Approval(s) required	Academic Senate ☐ Board of Trustees ☒ Both ☐
Date of Senate approval if required	(dd/mm/yyyy)
Date of Board approval if required	(06/12/2023)
Effective date of implementation	(06/12/2023)
Frequency of review required	Annually
Replacing or superseding information	
Revision number	New
Responsible Office	Office of Information Technology
Accountable Officer	Vice President Information Technology/Chief Information Officer
Related legislation, regulation, policy, or policies	Policy on IT Acceptable Use
Appendix/Appendices	Appendix A: IT Asset Deployment & Return Form Appendix B: University-Owned Mobile Devices Preferred Carriers Appendix C: University-Owned Mobile Devices Approved Software

1. **Authority**

Board of Trustees.

2. **Purpose**

The purpose identifies the policy goals.

3. **Scope**

This policy applies to all permanent, contractual, and temporary employees of the University of The Bahamas and any other third parties using equipment provided by the University of The Bahamas.

This policy applies to any mobile device that is used to access IT resources managed by the University of The Bahamas, is used to conduct University business, or is owned by the University. This includes, but is not limited to mobile phones, including non-internet connected devices; tablets, including Wi-Fi and SIM-connected devices; and laptop computers.

4. **Definitions**

Mobile Device: For the purpose of this policy, a mobile device is a small form factor, typically handheld, electronic device with at least one wireless network interface for network access for data communications. This interface can use Wi-Fi, cellular networking or other technologies to connect to the Internet or other data networks. The device contains local non-removable data storage and an operating system (OS). Mobile devices can include but are not limited to:

- Smartphones and cellular phones
- Tablets, Apple iPads and iPods
- Laptop computers

University-Owned Mobile Device: Broadly defined as any mobile device that is the property of and is maintained by the University of The Bahamas for business purposes. This includes all mobile devices purchased by a UB budget regardless of funding source, and whether purchased directly or through a reimbursement, or otherwise designated as UB property such as through a donation.

Eligible User: Users eligible for assignment of a UB-owned mobile device including:
UB employees (full-time, part-time, contractual, temporary) whose jobs require that they

- use a mobile device in their day-to-day activities
- must be reachable immediately
- are on call outside of normal business hours
- are often not based at a fixed work place and need to be easily contactable
- make frequent and/or prolonged travel outside of their home campus

Consultants, trainers and other third parties providing support to the University and requiring a UB-owned mobile device for connecting to UB internal networks in order to provide that support.

Device Holder: The individual to whom a UB-owned mobile device has been issued according to the guidelines set out in this policy.

Internal Networks: UB Wide Area (WAN), Local Area (LAN), Virtual Local Area (VLAN), and Wireless (WiFi) Networks – The computer networks maintained by the University of The Bahamas that interconnect computers within and between UB campuses allowing for the sharing of software, network storage and peripheral devices such as printers.

5. Policy Statement

5.1. Deployment of UB-Owned Mobile Devices

5.1.1. Assignement of Devices

5.1.1.1. Employment at the University of The Bahamas in any capacity at any level does not automatically guarantee the assignment of a University-owned mobile device

5.1.1.2. Mobile devices will be assigned to an employee, at the request of the department head and with the approval of the Dean/Vice President, based on the employee's job requirements and not his/her job title, position, level or rank.

5.1.1.3. UB-owned mobile devices may be assigned, on a short-term basis, to employees or consultants, as necessary, during specific assignments and projects.

5.1.2. Financial Feasibility

5.1.2.1. The deployment of mobile devices occurs dependent on the financial feasibility based on the current agreements in place. The cost of adding any additional devices to an existing plan for voice and data services must be reviewed and fall within allowable budgets of the requesting department and/or the Office of Information Technology before a new device is approved.

5.2. **Appropriate Use of UB-Owned Mobile Devices**: Mobile devices and services used to conduct the University's business must be used appropriately, responsibly and ethically. Failure to do so will result in immediate suspension of that user's account and/or confiscation of the mobile device.

5.2.1. Device Holder's Responsibilities

5.2.1.1. Individual users are responsible for:

- Using a non-trivial password and/or biometric authentication as supported by the mobile device;
- Keeping passwords secure and not sharing or disclosing device passwords;
- Enabling timeout or switching to a locked screensaver after less than 15 minutes of inactivity, with a password required to unlock the device;
- Using secure network connections that are encrypted and require authentication, when possible;
- Maintaining the software configuration of the device (i.e., operating system or installed applications);
- Using the mobile device in a lawful and responsible manner to avoid placing the employee or the organization in a position of liability for civil or criminal penalties (e.g., not taking unauthorized photographs or recordings);
- Protecting the physical security of the device; and
- Reporting the loss or theft of a mobile device immediately as outlined in this Policy.

5.2.1.2. UB-owned or private devices may only connect to UB's internal networks and related infrastructure using a UB-assigned user name and password combination.

5.2.1.3. UB-owned mobile devices are the property of University and must be treated, used and safeguarded as such. If a user damages or loses the issued device, a "Repair/Replacement form" (available from the University's website or the IT Help Desk) must be completed, with the appropriate signatures. The form must be submitted to the Office of Information Technology (OIT), along with the device, where possible.

5.2.1.4. Software installation, removal, or configuration modifications or hardware modifications to mobile devices should be made only by OIT staff. Such amendments must be in accordance with existing policies.

5.2.2. Use of Mobile Devices While Travelling Overseas

5.2.2.1. When traveling overseas, users must turn off "Data roaming" on the mobile device. Because there are additional costs associated with outgoing calls, data usage and text messaging outside of the local network (Be Aliv/BTC), users are asked to make use of Wi-Fi when available, and exercise discretion when making calls or sending text messages. In cases where the use of a mobile network is unavoidable for business purposes please connect to preferred carrier as outlined in Appendix D.

5.2.3. Use of UB-Owned Mobile Devices for Personal Activities

5.2.3.1. The use of institutional mobile devices for personal calls, texts and other applications is allowed if such usage is not excessive in frequency and duration or in breach of this or any other UB policies.

5.2.3.2. Authorized users must realize that although personal calls may not result in direct monetary charges, they do count toward the overall time limits established under the service agreements with voice and data service providers. Any substantial usage in excess of plan limits, including long-distance, data-use, roaming, or other charges incurred by the authorized user for personal purposes shall be the responsibility of the individual. The individual will be expected to reimburse the University, monthly, for such overages.

5.2.3.3. Use of UB-owned mobile devices for unlawful activities, commercial purposes unrelated to the University or for personal gain is forbidden. The use of a mobile device is subject to the University's IT Acceptable Use policy.

5.2.4. Reporting Inappropriate Use of UB-Owned Mobile Devices

5.2.4.1. Proof or justifiable suspicion of unauthorized access to UB systems, or illegal or inappropriate activity using the assigned mobile device will result in immediate confiscation of the device and removal of UB systems access. Any breach or suspected breach of the University's IT Acceptable Use Policy should be reported to OIT, through the IT Help Desk, for investigation. OIT reserves the right to perform in-house or third-party access audits/computer forensics to verify the occurrence and severity of a breach.

5.2.4.2. OIT reserves the right to recall an issued UB-owned mobile device periodically for audits or inspection.

5.2.5. Return of Issued Mobile Devices

5.2.5.1. Mobile devices and service that are purchased and maintained with university funds are the property of the University of The Bahamas. All university-owned mobile devices are to be returned to the OIT when an employee transfers to another department or otherwise separates from the institution.

5.2.5.2. The issued mobile device, including all issued accessories, must be returned to the user's department head along with a completed IT Asset Deployment & Return Form (available from the University's website or the IT Help Desk) in the following cases:

- The device holder's department head determines that the device holder's job no longer requires the use of the mobile device.
- The device holder is on extended leave and his/her department head decides to recall the device for the period of the leave.
- The device holder separates from the University for any reason including:
- Resignation
- End of contract
- Termination
- Death

5.2.5.3. In the event of the device holder's death, the department head is to arrange the recall of any mobile device issued to the user.

5.2.5.4. If the device and any included accessories are not returned in good working condition, the user may be asked to pay for the repair or replacement of the device and included accessories. Any associated service plans will be discontinued. Refer to the University's Exit Process for further details.

5.2.5.5. Mobile devices typically hold personal information, such as contact information for family and friends, call history, personal photos, stored passwords, and potentially sensitive data. As such, the device holder should take following basic steps prior to returning the mobile device:

- Transfer personal files, photos, contact information, etc. to another device or external storage.
- Clear the mobile device by initiating a "factory reset". Follow the instructions in the mobile device manual or on the website of the mobile device manufacturer.
- Double-check to make sure all personal information has been removed, including apps that you might have downloaded and installed.

5.2.6. Financial Impact

5.2.6.1. Mobile device service plans (data and voice) are to be reviewed periodically or on the introduction of new mobile device plans to determine if the plans are meeting the needs of the University.

5.2.6.2. The Office of Information Technology will be responsible for the cost of the initial device, once approved. This cost will cover an approved model of mobile device, and where applicable, the cost of the SIM card and associated services.

5.2.6.3. The Office of Information Technology will not be responsible for supplying any accessories other than the components included with the mobile device at the time it is issued. Non-included accessories such as protective cases, screen protectors, hands-free devices, spare batteries, etc. must be separately obtained by the user with personal funds.

5.2.7. Replacement of Mobile Devices

5.2.7.1. The cost of replacement of mobile devices may be borne by OIT in the following situations:

- In cases where the device is stolen, OIT will only cover the cost of replacement if the theft has been duly reported to the police and a copy of the police report is submitted to OIT
- Devices needing replacement through normal use (aged or outdated technology, system fault, failed battery) may be paid for through the affected department or the Office of Information Technology only when both Vice Presidents are in agreement on who shall assume the cost.
- In cases of urgent need of OIT-approved replacement where no funds are available in OIT's budget, the VP responsible for the affected area in consultation of VP Finance may use the option of transferring such funds to OIT's budget.

5.2.7.2. The device holder may be required to pay for the replacement of the device in the following situations:

- The device has been damaged through negligence for example where the device was dropped, has water damage, is lost or made otherwise unusable while the device is assigned to the user.
- The user requires the replacement of a mobile device more than once within three calendar years where the need for replacement is not due to a manufacturing fault.

5.2.7.3. The responsibility for the cost of replacement of mobile devices will be at the discretion of the Vice President for the affected department. Where an employee is responsible for replacing the mobile device, arrangements can be made with the Business Office and HR for the appropriate salary deductions as may be required.

5.2.8. Use of Personal Mobile Devices

5.2.8.1. Allowances may be made for employees who wish to use their personal devices for voice and data service to conduct UB business with the understanding that the employee must adhere to the same rules governing acceptable use for UB-owned equipment. These arrangements must be made at the discretion of the user's unit head with the approval of the VP responsible for that unit.

5.2.8.2. Stipends for voice/data services:

- Stipends may be paid to employees once per month
- Stipends are not to exceed $40 per month for voice and data messaging only except where specific approval has been granted in writing to exceed this amount.
- Stipends can be canceled at the discretion of the user's unit head or Vice President if it is determined that the arrangement is no longer needed, there is evidence of abuse or the employee's responsibilities no longer require the service.

5.2.8.3. The University does not accept liability for the maintenance, backup, or loss of data stored on users' personal mobile devices.

5.2.8.4. The University is not liable for the loss, theft, or damage of any user's personal mobile devices, including, but not limited to when the device is being used for University business or during business travel.

5.2.8.5. The User's personal mobile device may be subject to disclosure in the event of litigation, and the User will be required to cooperate with the University in providing access to the device for that purpose.

5.2.9. Monitoring and Confidentiality

5.2.9.1. Mobile device(s) and services are the property of the University of The Bahamas, who has the right to monitor any and all activities through its device(s).

5.2.9.2. All email messages and documents, both active in mailboxes, mobile devices and archived on storage media, are the property of the University. The University retains the right to access any and all email messages and documents as it becomes necessary.

5.2.9.3. Further, any archival and backup copies of email messages and documents may exist, despite the employee deleting them, which is a requirement of the records retention policy.

5.2.9.4. Back-ups exist primarily to restore service in case of email system or device failure. Back-ups and archives are governed by the University's document retention policy.

5.2.9.5. Employees should use extreme care when communicating confidential or sensitive information via mobile devices. If it is suspected that an employee is non-compliant with the University's policies, their device may be retrieved ensuring the employee is given due process.

5.2.10. Device Lifecycle

5.2.10.1. Mobile devices covered under this policy will be in circulation for a period of at least three years before being deemed out of cycle/standard. Mobile devices will only be replaced based on OIT's recommendations in accordance with section 8.4.1.2 of this policy.

5.2.10.2. For any replacement of devices within the three-year timeframe, please see section 6, Financial Impact, for the appropriate action.

6. History

The history table documents significant changes so that the evolution of the policy is recorded.

Revision	Date	Changes to Policy/Comments
new	13 Feb 2020	