STAFF MOBILE DEVICES POLICY

PURPOSE

The use of mobile devices is an important part of work requirements for some employees at Brock University. The purpose of this policy is to set out expectations around the provision and responsible use of mobile devices for Brock employees to support the effective operations of the University.

SCOPE

This Policy applies to the provision, use, administration and oversight of mobile devices owned or paid for by the University for Brock employees. It does not apply to the provision, use and administration of mobile devices by Brock University faculty and Professional Librarians.

If any provision of this Policy is found to be inconsistent with the provisions of a collective agreement, the collective agreement will prevail, unless the Policy provision is required by law, in which case the Policy provision will prevail.

POLICY STATEMENT

Device Eligibility

Brock may provide university-owned mobile devices, or partial reimbursement for employee-owned devices, to staff who meet the following criteria:

- Their defined role supports critical services and are required to be reached immediately;
- Not usually at a fixed work station and provides support where rapid response is often required;
- Is in a role requiring frequent travel and mobile connectivity; or,
- Demonstrates a need to have mobile access to critical information, documents, or communications.

University-Owned Devices

A Brock staff member may be assigned a university-owned mobile device based on the device eligibility criteria and the approval of their immediate supervisor / manager and Senior Administrative Council (SAC) member. Any role requiring

assignment of a University-owned device should be noted in the position's job description.

Employees with University-owned devices should ensure connection to wifi networks whenever feasible to do so, especially while on Brock campus or while travelling, in order to avoid data use overages and additional costs.

Employee-Owned Devices (BYOD)

Brock staff may be approved to receive partial reimbursement for an employee-owned device that is used for work purposes. Staff may be considered eligible for reimbursement if they meet the device eligibility criteria and receive approval from their direct supervisor / manager and SAC member. Brock staff may receive reimbursement equal to the value of the basic monthly Voice and Data plan for University devices.

Device Security

All University-owned mobile devices must be secured using a PIN or other password protection. Automatic lockout must be enabled for 5 or fewer minutes of inactivity. Any lost or stolen devices must be immediately reported to the employee's supervisor and ITS.

When a Brock employee is using a personal device for work purposes, they are responsible for ensuring good mobile device security practices. Users of personal devices for Brock work purposes must ensure device software is fully patched and up to date. Brock also encourages employees to use encryption on their devices where reasonable and appropriate to do so.

Device Upgrades

Where an upgrade of a University-owned device is required, for example if an advanced user requires more capability than a basic device offers, or if no free devices are available or included through the device provider program, an employee must obtain approval from their respective SAC member.

Employees may also choose to upgrade the cost of a device at their own personal expense. This should be discussed and agreed upon with the employee's direct supervisor and approved by the SAC member.

Personal Usage of University-Owned Devices

Employees assigned a University-owned device to their care are expected to use it in an appropriate and responsible manner. Employees are expected to reimburse the University for any personal use that results in additional charges as a result of exceeding the voice, data and text plans limits.

Travel Policy

The use of your mobile device outside of Canada for phone, data, or text messages services will result in extra charges to your account. These charges vary from country to country and are very expensive. Using your University-owned device 'out of country' is at the discretion of the employee's supervisor or direct report. Costs incurred without using the most economical method (ie. travel plan) and/or without prior approval will be the liability of the University-device user.

Roles and Responsibilities

Information Technology Services (ITS) is responsible for managing and administering the process around provision, use and security of University-owned mobile devices; managing the relationship with the approved vendor and ensuring agreements are up to date; ensuring that plans and devices offered are reasonable and appropriate; and for ensuring that all mobile devices used for University business have the requisite security protocols and controls set up.

Human Resources is responsible for ensuring device eligibility requirements are reasonable, appropriate, and updated as required, including incorporating technology requirements into job descriptions and organizational development as appropriate.

Users of University-owned devices are responsible for the appropriate use of devices assigned to their care. This includes ensuring compliance with this policy and the University's IT Appropriate Use Policy. Users are expected to take adequate precautions to guard against inappropriate usage and to protect the physical security of the device.

SAC Members and Department Managers are responsible for approving the provisioning of devices and reimbursement for BYOD and applying the principles of this policy and ensuring employees who receive a University-owned device or BYOD reimbursement meet the eligibility criteria of this policy. They

are also responsible for the oversight of the devices in their purview and for ensuring the reasonable and appropriate usage and allocation of University resources (devices or reimbursement $).

The President and Vice-Presidents are accountable for expectations of the University's Mobile Devices program and approval of this policy.

DEFINITIONS   **Mobile Device** refers to all cellular phones, smartphones, pager (if applicable) and all wireless data devices (tablets, USB modems, etc.) with a cellular/data subscription plan.

BYOD, also known as '**Bring Your Own Device**', refers to employee-owned devices that are used for business purposes and that the employee receives reimbursement for.

COMPLIANCE   The interpretation and application of this Policy is the
AND REPORTING responsibility of the Vice-President, Administration. Policy violations shall be reported to the Vice-President, Administration.

Policy Owner:	Vice-President, Administration
Policy Lead:	TBD by Vice-President, Administration
Policy Classification:	Operational
Approval:	Approved by the Executive Team
Effective date:	April 2021
Next review:	April 2024
Revision history:	New
Related documents:	N/A