CAPILANO UNIVERSITY	POLICY		
Policy No.	Officer Responsible		
OP.607	**Vice-President Finance and Administration**		
Policy Name			
Mobile Device Policy			
Approved by	Replaces	Category	Next Review
SLC		**IM&DT**	**December 2028**
Date Issued	Date Revised	Related Policies	
August 26, 2020	**December 13, 2023**	**OP.604 Acceptable Use and Security of Digital Technology Policy**	

1. PURPOSE

1.1 Capilano University (the "University") is committed to enhancing the ability of its community to communicate effectively and to foster a sense of community and learning.

1.2 This policy defines the terms and conditions used to determine who is eligible to receive a University funded mobile device and outlines the responsibilities with regards to the use of any mobile device that is used to access University resources, whether the device is owned by the employee or the University.

2. DEFINITIONS

"Employee" means any person employed by the University.

"Mobile device" in this policy refers to a smartphone.

"Personal mobile device" refers to a Mobile device which is wholly owned by the employee.

"University network" refers to any technology system or service provided by the University.

3. SCOPE

3.1 This policy applies to all Employees who use a Mobile device to access University resources; this includes University-owned devices, Personal mobile devices where the Employee receives a stipend for use and Personal mobile devices which are connected for the Employee's convenience and no stipend is provided.

4. POLICY STATEMENT

4.1 The University approves the use of Mobile devices where there is a defined business need, such as improved efficiency, increased service levels or where required for employee safety. The designation of roles as requiring the use of a Mobile device will be made by the respective Vice-President, or their designate.

4.2 Employees who are approved for a Mobile device may opt to receive a University-owned smartphone, or may participate in the University's Employee Owned Smartphone Program (also referred to as BYOD, or bring your own device). The Employee will receive a stipend of $60 per month for the business use of their device; participation in the Employee Owned Smartphone Program requires a signed Employee Owned Smartphone User Agreement. This reimbursement is considered by Canada Revenue Agency to be taxable income.

4.3 This policy also allows for an Employee not receiving a monthly stipend to connect their Personal mobile device to the University network, at their request and convenience. Providing this service incurs a licensing charge for the University's mobile device management software and mobile email access, which the University will cover. Employees are required to sign the Employee Owned Smartphone User Agreement before their device is connected.

4.4 Employees must adhere to all applicable laws regarding the use of mobile devices, regardless of device ownership, including restricting the operation or holding of mobile devices while driving; any imposition of a fine or demerit points to an employee's license as a consequence of any violation of the Motor Vehicle Act is the sole responsibility of the Employee.

4.5 The use of non-sanctioned mobile devices to backup, store or otherwise access any University data is strictly forbidden; this is to ensure the integrity and security of the University's network and technology resources.

4.6 Each Vice-President, or their designate, will be required to review their respective list of CapU funded mobile devices on an annual basis to authorize their continued use.

4.7 Employees who are approved for a smartphone and do not participate in the Employee Owned Smartphone Program (i.e. employees who have a University-owned smartphone) may elect to use their University phone for personal use, provided such usage does not incur additional costs to the University or violate any University policies including but not limited to OP.604 Acceptable Use and Security of Electronic Information Technology Policy. Any personal usage costs in excess of $10 in a month must be repaid to the University.

4.8 When an Employee who has been provided with a University-owned smartphone ceases employment with the University, the Employee may request to transfer their mobile phone number to a personal account, or to the account of their new employer. This request must be approved by the respective Vice-President.

Personal Mobile Devices

4.9 The following guidelines apply only to Employees using a Personal mobile device:

a) Employees are responsible for any costs above and beyond the monthly stipend provided by the University, including ongoing costs, maintenance, repairs or replacements, accessories, carrier contracts and maintaining the functionality of the device in the University's environment. Unique situations, such as extraordinary roaming requirements, will be handled on a case by case basis and must be approved by the employee's administrator in advance.

b) Where an Employee receives a monthly stipend, the Employee agrees to the use of their Personal mobile device for University purposes, in the same way as they would a University-owned device. This includes consenting to the use and disclosure of their mobile phone number for business purposes in the same way a University-owned mobile number would be disclosed.

c) Employees choosing to use a personal smartphone device are expected to provide an advanced level of self-support, and the IT Services department will provide support only as it relates to University applications.

d) Where an employee receives a monthly stipend, IT Services will provide the employee with a loaner device in the event of loss, theft or equipment failure for a maximum of one month; if the employee is unable to replace the device, their participation in the Employee Owned Smartphone Program ceases and they will be provided with a University-owned device and they will no longer receive a stipend.

e) An employee may switch between the Employee Owned Smartphone Program and having a University-owned smartphone no more than once per year, in order to minimize administrative costs.

f) If an Employee in the Employee Owned Smartphone Program ceases University employment, they must allow University IT staff access to remove all University applications and data, including University email and calendars from their Personal mobile device.

5. SECURITY

5.1 The University reserves the right to prevent access to the University network or services by any device that is considered a risk. Employees understand that by attaching a Personal mobile device to the University 's network or services, they are accepting responsibility for protecting access to University data. Devices must meet the minimum security requirements required by IT Services (this covers most Android and Apple devices) and a device connected to the University's network must not be loaned to non-University employees under any circumstances.

5.2 To secure protected information, the University will install mobile data security software on all University owned devices and reserves the right to install mobile data security software on Employee's Personal mobile devices following a request to connect to the University network. In exceptional circumstances the University may require access to University information on an Employees Personal mobile device or require that data on an Employees Personal mobile device be remotely wiped (e.g. in the event of loss or theft of the device. It is the responsibility of the Employee to report instances of loss or theft to the University in a timely manner. This software is used only to preserve the integrity and security of the University's records and network and is not used to track the Employee's location or to log or monitor phone calls, text messages or other phone usage.

6. DESIGNATED OFFICER

The Vice President, Finance and Administration is the Policy Owner, responsible for the oversight of this Policy. The Administration of this Policy and the development, subsequent revisions to and operationalization of any associated procedures is the responsibility of the Associate Vice President Digital Technology Services.

7. RELATED POLICIES AND GUIDANCE

OP.604 Acceptable Use and Security of Digital Technology Policy

Employee Owned Smartphone Agreement