Updated April 2024

Procurement and Use of Stevens Cellular Devices Policy

Approval Authority	**Cabinet**
Responsible Officers	**Chief Financial Officer, Vice President for Finance and Treasurer** **Chief Information Officer, Vice President for Information Technology** **Senior Vice President for Academic Affairs and Provost**
Responsible Offices	**Division of Finance** **Division of Information Technology** **Office of the Provost**

Effective Date: March 1, 2024

A. Purpose of this Policy

The purpose of this policy is to outline appropriate use and security for both Stevens-provided and personally-owned cellular devices, and to establish a framework for consistent decision-making regarding the provision of essential, business-related cellular devices to Stevens Institute of Technology (Stevens) faculty and staff (employees). This policy pertains to those cellular devices that require contracts with a cellular network provider. Cellular devices may include cellular phones and smartphones that use a cellular wireless network for communications. Sections B. through G. of this policy pertain to the use of Stevens-provided cellular devices for business purposes. Section H. pertains to the use of personally-owned devices which are used for university business purposes.

B. Eligibility for Stevens-Provided Cellular Devices

Stevens-provided cellular devices may be necessary for employees to perform their job requirements in a responsive and efficient manner. These employees typically need to be contacted regularly for work-related issues outside of normal business hours.

Senior level leadership are eligible for Stevens-provided cellular device(s) to facilitate the conduct of Stevens' business.

Stevens will follow the Internal Revenue Service (IRS) guidelines below to establish whether an employee may require a Stevens-provided cellular device.

- The need to contact the employee at all times for work-related emergencies.
- The requirement that the employee be available (i.e., "on-call") to speak with donors, applicants, students, or other constituents at all times when the employee is away from the office.
- The need for business conversations with individuals in other time zones at times outside the employee's normal workday.

A general business need to remain in contact with Stevens or to monitor ongoing communications related to one's duties is not a sufficient standard for the issuance of Stevens- provided cellular devices and/or exclusion from income taxes. Eligibility should be determined based on the frequency of the use of a cellular device for business purposes.

All Stevens-provided cellular devices are to be used for campus business. If the device is used for casual, personal, or incidental use and incurs extra charges, those charges must be reimbursed or paid directly by the employee.

C. Routing and Approvals

Divisional Vice Presidents are responsible for determining eligibility and initiating a request using the Cellular Device Request Form in consultation with the Chief Financial Officer, Vice President for Finance and Treasurer. The Chief Financial Officer, Vice President for Finance and Treasurer will review and approve requests for administrators and staff. The Senior Vice President for Academic Affairs and Provost will review and approve any requests for faculty and academic leadership. The Cellular Device Request Form can be accessed at www.stevens.edu/cellulardevicerequest.

D. Stevens-Provided Cellular Device and Service Plan

Once approval is granted for an employee to receive a Stevens-provided cellular device, the device will be enrolled in a Stevens plan which will be limited to the cost of basic equipment and service. Plan service levels shall be consistent with the employee's anticipated business use. Stevens will not fund any accessories and applications that are purchased for a Stevens-provided cellular device. Equipment upgrades beyond the basic level and any accessories shall be paid by the employee using personal funds. Divisional management shall monitor the cell phone usage and the employee's business responsibilities at least annually to ensure that the charges are reasonable and that job responsibilities continue to meet IRS criteria.

Stevens-provided cellular devices are the property of the University. When the employee separates from Stevens, or transfers to a different organization within Stevens, the supervisor shall immediately deactivate the employee's account and the employee must either purchase the cell phone at fair market value as determined by the Division of Information Technology (IT) or return the equipment to Stevens. In either case, the employee may be given the option to retain the phone number affiliated with the device.

E. Cellular Device Usage

Employees are responsible for taking reasonable care of their cellular communications devices. If an employee's device is lost, damaged, or destroyed through negligence, the employee may be required to repair or replace it at their expense. Employees are responsible for immediately reporting any loss or theft of an institutionally supported device to the Division of Information Technology – Office of Information Security Services. To report a lost or stolen cellular device, use the instructions on the Stevens Support Portal.

F. Safety

Employees are expected to follow all applicable local, state, and federal laws and regulations regarding the use of cellular devices at all times. Employees must refrain from using their devices while driving regardless of the circumstances, including slow or stopped traffic. Employees are required to use hands-free-enabled technology or safely stop a vehicle before placing or accepting a call, texting, or emailing. Special care should be taken in situations involving traffic, inclement weather, and unfamiliar geographies. Employees who are charged with traffic violations resulting from the use of their devices while driving will be solely responsible for all liabilities that result from such actions.

Employees who work in hazardous areas, such as laboratories, must refrain from using cellular devices while at work in those areas.

G. Security

All Stevens-provided cellular devices must be configured to lock with a password or PIN if the device is idle for two minutes. Employees are not allowed to circumvent built-in device security controls (e.g., changing passphrase/PIN lengths, authentication requirements).

Employees should apply updates and patches to their cellular device's operating software to mitigate security threats. This can be done by enabling automatic updates, or accepting updates when prompted by the device manufacturer, operating system provider, service provider or application provider.

If a device is lost or stolen, the employee must promptly notify the Office of Information Security Services at security@stevens.edu to reset device. To report a lost or stolen cellular device, use the instructions on the Stevens Support Portal.

Accounts used to set up cellular device app installations and downloads should be created for the sole purpose of a Stevens cellular device and should not be the individual's personal account (e.g., Google or Apple account). This ensures that no Stevens data is inadvertently synced to other personal devices and that sensitive personal information is not on the Stevens cellular device.

All Stevens-provided cellular devices should comply with best practices for securing cellular devices (see Appendix A).

H. Use of Personally-Owned Devices for University Business

i. Enforcing Security

All personally-owned cellular devices which are used to conduct Stevens' business shall be used in accordance with this policy and subject to minimum security requirements which can be found at stevens.edu/security. Examples include using a personally-owned device to access Stevens' email (including web-based e-mail applications) or Teams, Zoom or other business platforms (e.g., Canvas and Workday).

All personally-owned cellular devices used for university business should comply with best practices for securing cellular devices (see Appendix A).

ii. Device Protocols

Stevens requires certain personal cellular device features to be enabled to support prudent device protection. Specifically, the device must be configured to lock itself with a password or PIN if it is idle for two minutes.

Employees are not allowed to circumvent built-in device security controls (changing passphrase/PIN lengths, authentication requirements).

Employees should accept updates and patches to their cellular device's operating software to mitigate security threats. This can be done by enabling automatic updates, or accepting updates when prompted by the device manufacturer, operating system provider, service provider or application provider.

iii. Privacy/University Access

Employees are entitled to privacy on their personal devices. However, such privacy does not extend to Stevens' data and related applications, or privacy-related disclosures governed by law. Therefore, Stevens has the right, at any time, to require an employee to produce a cellular device which is used for Stevens business purposes and preserve materials on such device for legal purposes.

iv. Lost, Stolen, Hacked or Damaged Equipment

Employees are asked to immediately report a lost or compromised device, whether personally or Stevens-provided cellular devices, to the Division of Information Technology – Office of Information Security Services. The Office of Information Security Services will promptly take action to mitigate the related risk. The University will not assume responsibility for costs associated with repairing or replacing a personal device. To report a lost or stolen cellular device, use the instructions on the Stevens Support Portal.

The Office of Information Security has the authority to use software to remotely wipe out a device's institutional-related data to protect sensitive institutional data in the event the device is lost or stolen.

v. Disposal of Device

Employees should take every precaution to secure Stevens' data should they decide to dispose of their device. Employees should perform a factory reset or remove all Stevens-related data prior to disposal.

vi. Termination of Employment

Upon termination of employment, as outlined in the Employee Handbook (section 4.10), Human Resources will promptly notify the manager and IT department. IT will then ensure the removal of all institutional data from personally owned devices, either upon resignation or termination of employment, or at any time upon request. Additionally, it is the employee's responsibility to uninstall all Stevens-related applications from their personal devices.

vii. Reimbursement of Cellular Device Voice/Data Plans

Stevens does not reimburse employees for personally-owned cellular devices and/or their usage.

Appendix A: Best Practices for Securing Cellular Devices

Cellular devices refer to smart phones, tablets, and e-readers. Users with cellular devices that are either Stevens-provided cellular devices or personally managed need to ensure the following:

1. Use a strong passcode to lock your device. Consider using biometrics authentication (e.g., fingerprint, face) for convenient data protection.
2. Update your operating system regularly. For convenience, consider turning on automatic software updates.
3. Do not jailbreak/root your cellular device. You may stop receiving important security updates and the device will become more vulnerable.
4. Enable encryption on your cellular device. iPhone and Android have built-in encryption, and enablement options can be found in the device settings.
5. Wipe or securely delete data from your cellular device before you dispose of it. Additionally, unlink your Okta Verify MFA.
6. Notify IT immediately if your Stevens-provided cellular device or personally-owned device used for University business is lost, stolen, or misplaced. To report a lost or stolen cellular device, use the instructions on the Stevens Support Portal.

These best practices should be used for all devices used to connect to Stevens' email or systems.