Purchase College Mobile Computing Device Usage Policy

Purpose

This policy offers some best practices regarding the use and safekeeping of laptops, tablets, and mobile computing devices, and governs the use of and liability for College-owned mobile devices.

What's covered by this document?

All College-owned mobile computing devices are governed by this policy, including systems made available as primary workstations, assigned within a departmental office, or purchased through grant dollars for specific projects.

All college-owned computers, systems, and mobile devices are covered by the Purchase College Privacy Policy which provides protection for individual privacy appropriate for an academic environment.

Scope

This document is applicable to all College staff, faculty, or administrators who are using mobile computing devices issued or loaned to them by a College department.

College-owned mobile devices may be used for any work-related tasks, including:

- as your primary workstation.
- on a College trip, conference, or workshop.
- for research, creative production, or any work-related purpose.

General Use

- You will receive administrative credentials for your device.
- Feel free to change user settings to your liking
- Please be sure to safeguard the device - log off or "lock" the device when it is not in use.

Physical Protection and Reasonable Care

- Password protect all mobile devices
- Secure your mobile device and keep it with you.

Reporting Loss

- Report a theft immediately to:
  - The appropriate local law enforcement authority
  - Purchase College University Police
  - CTS (Helpdesk 914.251.6465) as soon as the theft has been noticed. Provide CTS with a copy of the police report.

General information on Faculty Computers and Mobile Devices

Acquisition

- Administrative units provide their staff with computers, laptops, and mobile devices as necessary.
- Academic Affairs provides faculty computers, laptops and mobile devices for all faculty as necessary.

Inventory, Reporting, and Replacement

- Each year, CTS produces a report for Academic Affairs showing all full-time faculty computers as recorded in the College's Workstation Database.
- The CTS report shows all faculty computers (desktops and laptops), with "replace" recommendations in cases where an individual's only workstation is outdated or out of warranty, or where all of that individuals computers are outdated or out of warranty. Replace recommendations are for a like device (desktops replaced with desktops).
- The report to the Provost is accompanied by an overall cost estimate based on a current quotation for the mix of desktops/laptops covered by the "replace" recommendations.
- Academic Affairs may solicit input from Chairs/Directors regarding pending personnel changes and/or the appropriateness of each "replace" recommendation.
- Chairs/Directors may solicit feedback from individual BOS or faculty within their unit.
- Academic Affairs returns a final "replace" recommendation containing the names and types of devices (Mac or PC, desktop or laptop) to CTS for ordering.

Preparation for use:

- Upon arrival, CTS prepares the machines by joining them to the college network and loading college software onto them.
- CTS notifies each faculty member when their device is ready for delivery or pickup.
- Upon delivery/pickup of a new device, the device being replaced must be returned to CTS. Data can be transferred to the new device during the handoff.
- Administrative access is provided for all mobile device holders. Administrative access allows you to access the mobile device when it is not connected to the college network (offsite), to change settings, install software and apply updates, and other functions.
- College credentials (CTS) will exist on all College-owned devices to enable CTS staff to provide support and maintenance services as needed.
- Upon resignation or departure from College service, all College-owned equipment –must be returned to CTS for inventory purposes, reassignment and/or disposal. All data is wiped from computing devices prior to disposal.

Physical Protection and Reasonable Care

- Every mobile computing device must be password-protected
- Each user of a College-owned mobile device is responsible for the security of that device, regardless of whether it is used in the office, at one's place of residence, or in any other location such as a hotel, conference room, car or airport. Users are expected to provide reasonable care and effort to protect the mobile device.
- The equipment may not be transported as checked luggage on public transportation (airplanes, trains, and buses). The user will keep the equipment in their possession at all times while traveling.
- Carrying cases and mobile devices should be labeled accordingly so in the event of a loss the equipment might be returned. All mobile devices must have a College asset tag.

- Special care should be taken with the security of the mobile device. Equipment must not be left unattended in public areas. Do not leave your office unattended and unlocked, even for a brief time, if your mobile device is not secured in the office.
- Do not store mobile devices in a locked car or car trunk, as severe temperatures may damage it and the car may be broken into if the mobile device can be seen.

Liability

Along with the privilege of using a College owned mobile device comes the responsibility to safeguard the device and any data it contains.

- Individuals are personally responsible for the security and safety of the mobile device.
- Departments should not loan college-owned mobile devices to students, student organizations, or other outside parties. CTS maintains a distinct pool of equipment for this type of use, and requests should be referred to CTS.
- In case of theft or loss, the employee must file a report with the University Police.
- A theft must be reported immediately to:
  - The appropriate local law enforcement authority
  - Purchase College University Police
  - CTS (Helpdesk 914.251.6465) as soon as the theft has been noticed. Provide CTS with a copy of the police report.
- If a mobile device is damaged, lost or stolen and it is determined that reasonable care and protection guidelines were not followed, the person to whom the mobile device was may be subject to disciplinary action. The determination of responsibility will be made by a College Officer, in consultation with the unit supervisor, UPD, CTS and the Property Control Officer.
- Failure to follow this policy and these procedures may result in loss of computer privileges.
- Failure to return the mobile device may result in disciplinary or legal action.
-

Data Security

Data Security policies apply to all computing devices used for College business. Since mobile computing devices are more susceptible to loss or theft, it is important that you **do not store any Personal Private Sensitive Information (PPSI) on mobile devices,** and that you **maintain current backups of any important files** that you do have on the mobile device**.**

Why avoid storing personal, private, and sensitive information? Mobile devices are particularly susceptible to loss or theft. If Personal Private Sensitive Information (PPSI) is stored on a device that is lost or stolen, the individuals whose information was compromised may face long lasting ramifications from the improper use of their personal and financial information. In addition, New York State law may require that the college publicly disclose the loss of such PPSI and notify all individuals whose information was potentially compromised. As a result, we highly recommend that you **do not store any sensitive data on mobile computing devices.**

What is Personal, Private, and Sensitive Information (PPSI)?

Per NYS Cyber-Security Policy P02, PPSI is considered a combination of any three of the following personally identifiable information items: Name, Address, SSN, account number, credit card number, maiden name, and date of birth.

To Secure Data on Your Device:

- Ensure that virus protection updates, operating system updates and virus scans are performed regularly (these are default CTS settings.)
- When using your mobile device in a public place, use encrypted network connections (via HTTPS on Wi-Fi or VPN) to ensure your communications remains secure.
- Avoid using "remember me" for websites that require an account log on. This avoids storing your ID/password for that site in cookies and browser cache files.
- Do not download, store, or record data that includes any personally identifiable information such as: student/faculty/staff/alumni/vendor Name, Address, SSN, account number, credit card number, etc. If the mobile computing device is lost or stolen, this data could be used for Identity theft. The user is responsible for the security of all College data stored on, or carried with, the mobile device.
- Do not alter any system software or hardware configuration unless instructed to do so by someone from Campus Technology Services.
- Additional application software should not be loaded onto the mobile device unless approved by Campus Technology Services.
- Safe guard the device and data by ensuring the mobile device is "locked" or the user is logged off when not in use.

Inventory Tracking and Disposal

- Upon termination of college employment, the mobile device, peripherals, and carrying case need to be returned either to the issuing department or to the CTS Helpdesk on or before the last day of work.
- Do not give the mobile device to anyone else for use. Doing so will be considered misuse of the equipment.
- The department responsible for the mobile device must maintain records of who has which mobile device for what period of time. The department responsible for the mobile device should retain a copy of each Mobile Device Authorization Form they issue. If the mobile device does not have a barcode, then the unique identifying number (e.g. a serial number or service tag number) should be used to identify the equipment.
- When a mobile device reaches the end of its useful life, it must be returned to the CTS Help Desk for disposal. They will ensure that the device is wiped clean before the unit leaves campus.

++

Failure to comply with this policy may result in disciplinary and or legal action.

Thank you for reading this document.

Acknowledgement of Mobile Computing Device Usage Policy

Purchase College / State University of New York

_____ authorize _____ to receive a mobile computing device.

(Supervisor's name) (Employee's name)

Mobile computing device information:

Laptop ___ Tablet ___ Other _____

Manufacturer _____ Model_____

Serial # _____ Original cost: _____ Date of purchase: _____

SUPERVISOR

I approve the issuance of a Mobile Computing Device to the employee: _____/_____

(Supervisor signature / date)

COLLEGE OFFICER

I approve the issuance of a Mobile Computing Device to the employee: _____/_____

(College Officer's signature / date)

•

EMPLOYEE:

I have read and agree to follow the Mobile Computing Device Usage Policy: _____/_____

(Employee signature / date)

Submit form to Campus Technology Services. A copy should also be retained by the issuing department.

This information has been recorded in the computer inventory database: _____

(CTS Reviewer / date)