

THE GEORGE WASHINGTON UNIVERSITY MEDICAL CENTER POLICY ON FACULTY/STAFF LAPTOP COMPUTERS

POLICY STATEMENT

The George Washington University Medical Center is committed to providing an appropriate computer system for each fulltime faculty and staff member. Computer systems are intended for use for university-related business as a productivity tool, curriculum tool, and for research and communication. It is not intended as a replacement for any computers that may be owned personally. Laptops are not to be used to house or manage confidential data as defined by the [Data Classification Security Policy](#). Examples but not all inclusive: student grades, student financial records, personal information of students, faculty, staff, alumni, or development prospects. Any laptop purchased with George Washington University funds, will be encrypted.

REASON FOR POLICY

This policy addresses the need by some faculty and staff members for a laptop computer instead of a desktop computer. The laptop program will enable faculty or staff of George Washington University to conduct university business from various off-campus locations.

WHO NEEDS TO KNOW

Faculty and Staff

POLICY/PROCEDURES

A University owned laptop is intended for use for university-related business. Use of a university owned laptop for personal purposes should be within the standards of good judgment and common sense, in compliance with the university's published policies [code of conduct for users of computing systems](#), and as required through the terms and conditions of applicable software license agreements. Technology support of university owned laptops will be equivalent to that provided for university owned desktop computers. Direct support will only be provided while laptops are on campus.

A. Eligibility

- Laptops will be allocated to users based upon job responsibilities, demonstrated need, and school/department approvals.
- Benefits-eligible faculty and staff of the University will be eligible for consideration for laptops. Neither adjunct faculty members nor vouchered

employees will be eligible for the faculty and staff laptop program at this time.

- Only one computer will be provided by the university for each faculty or staff member.
- Ownership of the laptop computer resides with the University and must be returned when employment ends.

B. Approval Process/Requirements

All requests for laptops must go through the assessment process via the Computer Applications Support Services (CASS) [assessment form](#). All orders for laptops (as any technology equipment or software) must be processed through CASS.

- Faculty/staff will need to state the reason(s) they are requesting a laptop, and what software and hardware needs they have.
- The laptop must be a configured, model and brand approved and must meet or exceed standard specifications. CASS will generate an E-Quote.
- The department is responsible for the purchase of additional office accessories such as monitor, keyboard, mouse, docking station, batteries or other consumables as may be needed.
- At the beginning of any replacement cycle, laptop users must re-apply for a laptop.

C. Faculty/Staff Responsibilities:

It is the faculty/staff member's responsibility to take appropriate precautions to prevent damage to or loss/theft of a university owned laptop computer. The faculty/staff member or department may be responsible for certain costs to repair or replace the computer if the damage or loss is due to negligence or intentional misconduct. Policies for appropriate use of university property as identified in the faculty/staff handbooks or elsewhere may be used to determine whether liability due to negligent behavior exists.

1. **Physical Security:** Physical security of the laptop is governed by the [Laptop Computer and Electronic Data Mobile Device Security Policy](#) and [Laptop Computer and Small Electronic Device Theft Policy](#). If a laptop is lost or stolen it must be reported to University Police immediately. For theft or loss off campus, it should be reported to local police as well. The police report should include the serial number for the lost/stolen computer. A copy of the police report must be sent to CASS within 48 hours of the discovery of the loss. Failure to secure and submit a police report will result in personal liability for replacement cost(s).
2. **Upgrades and Troubleshooting:** Faculty and staff are responsible for facilitating upgrades and troubleshooting. This may require that the laptop be brought to campus for hardware service, software installation or

problem diagnosis. CASS staff will not visit your home or go to non-Foggy bottom locations to provide service.

3. **Software Licensing:** The laptop will be configured with a standard suite of programs that are appropriate for the type of computer you received based upon the campus software standards. The laptop will also be encrypted to protect data stored on the hard drive. It is also possible that other applications will be provided to you by the University, based upon your professional needs or the requirements of the laptop. The university has policies for appropriate use of software, including the requirement to demonstrate legal license to a program before it can be installed on a university-owned computer. Faculty/staff will not be given administrative rights to the University-owned computers they use. You may not load games, entertainment software or personal finance software on a university-owned laptop computer.
4. **Backup:** Faculty/staff are responsible for maintaining an appropriate backup of their laptop, especially of the work-related documents and data files created that are not restored when reinstalling the operating system and programs. Depending upon the laptop, some documents and data files may need to be stored on the laptop's hard disk drive. It would be prudent to establish a process of copying the data files on the laptop to an assigned central data storage area (i.e., the George Washington server) as an added precaution against data loss. Use of central data storage for backup of personal documents or data files is prohibited.
5. **Virus, Hacking, and Security Protection:** To ensure that virus protection and other security patches are current, laptops must be connected to the University's network on a regular basis and faculty/staff must take responsibility for ensuring that security updates take place on laptops in their care. In the case of a significant security alert, users may be contacted by e-mail and/or voicemail, to bring in their laptops to the helpdesk to ensure proper security is enabled on the laptop. Although CASS pushes updates to university computers, laptops that are frequently off the university network may require manual updating. The user will be required to bring the laptop to the Foggy Bottom campus. For more specific guidelines refer to the [Laptop Computer and Electronic Data Mobile Device Security Policy](#).
6. **Off Campus Internet Access:** The University is not responsible for Internet service provider (ISP) access or connectivity. Users should feel free to connect the laptop to the Internet from locations other than campus, such as through an Internet service provider (ISP) at home. The laptop will be configured with a modem and Ethernet, two common ways to connect to the Internet through an ISP. CASS will neither provide Internet access to you from off campus nor configure your laptop to work with your ISP. Although CASS may offer some

tips or advice about best practices for off-campus use, it will be up to you and your ISP to make remote connections work.