Acceptable Use Policy
USG Policy 6 (1.00) | Approved by the Executive Director, May 2019

I. Purpose and Applicability

The purpose of this policy is to ensure the appropriate use of Universities at Shady Grove (USG) Office of Information Technology (OIT) resources while protecting the sharing of information, the right to privacy, freedom of expression, intellectual property, and security of information.

The scope of this policy includes any and all use of USG OIT resources including, but not limited to, computer systems and devices, software and application services, email and electronic messaging, the campus network, and the USG Internet connection. This applies to all populations including, but not limited to, students, staff, faculty, contractors, vendors, and all campus visitors/guests.

The Universities at Shady Grove is hereinafter referred to as "USG" and the Office of Information Technology as “OIT.” This policy will be reviewed annually to ensure continual compliance with USM OIT Security Standards and other pertinent policies, laws and industry standards.

II. Definitions

A. *Device*: Any portable or fixed computational machine with the capabilities of transmitting and/or receiving data over a wired or wireless network.

III. Policy Statement

A. Those using USG IT resources, whether on campus or elsewhere, are responsible for complying with security standards set forth by the Director of OIT and USG Senior Leadership, safeguarding identification codes and passwords, and for using them solely for their intended purposes. Individuals are solely responsible for their personal use of IT resources and are prohibited from representing or implying that statements related to such use constitute the views or policies of USG.

B. The maintenance, operation, and security of IT resources require responsible USG personnel to monitor and access systems and networks. To the extent possible in the electronic environment and in a public setting, a user’s privacy will be preserved. Nevertheless, that privacy is subject to applicable federal and state law, including the Maryland Public Information Act, and the needs of USG to meet its administrative, business, and legal obligations.

IV. Prohibited Content

A. The following provisions describe conduct prohibited under this policy:

1. Altering system software or hardware configurations without authorization; disrupting or interfering with the delivery or administration of IT resources.
2. Attempting to access or accessing another's accounts, private files, e-mail messages, or intercepting network communication without the owner's permission except as appropriate to one's job duties and in accordance with USG's legitimate purposes.
3. Misrepresenting oneself as another individual in electronic communication.
4. Installing, copying, distributing, or using digital content (including software, music, text, images, and video) in violation of copyright and/or software agreements or applicable federal and state law.
5. Engaging in conduct that interferes with others' use of shared IT resources.
6. Using USG IT resources for commercial or profitmaking purposes or to represent the interests of groups unaffiliated with USG or unassociated with the normal professional activities of faculty, staff or students without written authorization from USG.
7. Ignoring individual departmental or unit lab and system policies, procedures, and protocols.
8. Facilitating access to USG IT resources by unauthorized users.
9. Exposing sensitive or confidential information or disclosing any electronic information that one does not have the authority to disclose.
10. Knowingly using IT resources for illegal activities. Criminal or illegal use may include obscenity, child pornography, threats, harassment, copyright infringement, USG trademark infringement, defamation, theft, identity theft, and unauthorized access.

V. Enforcement

A. The enforcement of this policy will be carried out by authorized USG OIT personnel designated by the Director of OIT and USG Senior Leadership. Violations may result in disciplinary actions, which may include suspension, restriction, or revocation of access. Where illegal activities or theft of USG property (physical or intellectual) are suspected, USG may report such activities to the state/federal law enforcement authorities.

VI. Revision History

Date	Description	Revised By
11/27/2017	Initial Policy Creation	Russell Schlosburg

VII. Related Documents

A. USM IT Security Standards v4
http://www.usmd.edu/usm/adminfinance/itcc/USMITSecurityStandards.pdf

B. Maryland Public Information Act
http://www.marylandattorneygeneral.gov/Pages/OpenGov/pia.aspx