**Purpose:**

As part of its educational mission, the University of Florida acquires, develops, and maintains computers, computer systems and networks. These Information Technology (IT) resources are intended for university-related purposes, including direct and indirect support of the university’s instruction, research and service missions; university administrative functions; student and campus life activities; and the free exchange of ideas within the university community and among the university community and the wider local, national, and world communities.

**Scope:**

This policy applies to all users of university IT resources, whether affiliated with the university or not, and to all uses of those resources, whether on campus or from remote locations.

**Policy:**

**General Rules**

Users of university IT resources must comply with federal and state laws, university rules, regulations and policies, and the terms of applicable contracts including software licenses while using university IT resources. Examples of applicable laws, rules and policies include but are not limited to the laws of libel, privacy, copyright, trademark, obscenity and child pornography; the Florida Computer Crimes Act, the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, which prohibit “hacking,” “cracking” and similar activities; the university’s Student Code of Conduct; the university’s Sexual Harassment Policy; the University’s Policy on the Use of the University Name and Logos, the University’s Web Page policy, and the University’s Electronic mail Policy. Users who engage in electronic communications with persons in other states or countries or on other systems or networks may also be subject to the laws of those jurisdictions and the rules and policies of those other systems and networks. Users with questions as to how the various laws, rules and regulations may apply to a particular use of university computing resources should contact the Office of the General Counsel for more information.

Users are responsible for ascertaining what authorizations are necessary and for obtaining them before using university IT resources. Users are responsible for any activity originating from
their accounts which they can reasonably be expected to control. Accounts and passwords may not, under any circumstances, be used by persons other than those to whom they have been assigned by the account administrator. In cases when unauthorized use of accounts or resources is detected or suspected, the account owner should change the password and report the incident to the UF Computer Security Incident Response Team (ufirt@ufl.edu) and the Unit Information Security Manager.

Disruptive use of university IT resources is not permitted. Units administering the resources involved will determine whether specific usage is considered normal, excessive or disruptive. Although there is no set bandwidth, disk space, CPU time, or other limit applicable to all uses of university IT resources, the university may require users of those resources to limit or refrain from specific uses if such use interferes with the efficient operations of the system.

Employees may not use University IT resources to access or store pornographic material, except as may be specifically approved for limited research or business-related purposes.

Users may not use IT resources to gain unauthorized access to remote computers or to impair or damage the operations of UF computers or networks, terminals or peripherals. This includes blocking communication lines, intercepting or sniffing communications, and running, installing or sharing virus programs. Deliberate attempts to circumvent data protection or other security measures are prohibited.

Users who violate this policy may be denied access to university IT resources. The university may suspend, block or restrict access to an account when it appears necessary to do so: a) to protect the integrity, security, or functionality of university or other IT resources; b) to comply with legal or contractual requirements; c) to investigate alleged or potential violations of law or policy including, without limitation, state, federal, or local law, or university or Board of Governors rules, regulations, policies, or collective bargaining agreements; d) to investigate any asserted, threatened or potential complaint or grievance filed or credibly alleged pursuant to law or university or Board of Governors rules, regulations, policies, or collective bargaining agreements, or subject of law enforcement review or investigation; e) or to protect the university from liability or disruption. The university may also refer suspected violations of law to appropriate law enforcement agencies for further investigation or action.

Users who violate the Policy may be subject to other penalties and disciplinary action, including expulsion or dismissal, under applicable university or Board of Governors rules, regulations, policies, or collective bargaining agreements.
Policy: Acceptable Use

Security, Privacy, and Public Records

The university employs various measures to protect the security of its IT resources and user accounts. However, the university cannot guarantee complete security and confidentiality. It is the responsibility of users to practice “safe computing” by establishing appropriate access restrictions for their accounts, by guarding their passwords, and by changing them regularly.

Users should also be aware that their use of university IT resources is not private. While the university does not routinely monitor individual usage of its IT resources, the normal operation and maintenance of the university’s IT resources require the backup and caching of data and communications, the logging of activity, monitoring of general usage patterns and other activities necessary or convenient for the provision of service.

The university may monitor UFIT resources and retrieve communications and other records of specific users of UFIT resources, including individual login sessions and the content of individual communications, without notice. The criteria and steps required for approval of such monitoring or retrieval without notice are set forth in the Monitoring of IT Resources policy.

Communications made by means of university IT resources are also generally subject to the Florida Public Records Law to the same extent as they would be if made on paper. In this regard, university personnel and agents should be aware that most written communications concerning university matters, regardless of whether university computing resources are used, are public records, many of which are disclosable to the public upon request. Public records requests must be referred to University Relations or the Office of the General Counsel for coordinating the response and review of requirements and exemptions.

Retention periods must be followed for all university records and communications as required by the Florida Public Records Law and any other applicable law or contractual requirements.

Commercial and Personal Use

IT resources are not to be used for personal commercial purposes or for personal financial or other gain. Occasional personal use of university IT resources for other purposes is permitted when it does not consume a significant amount of those resources, does not interfere with the performance of the user’s job or other university responsibilities, and is otherwise in compliance with this and other university policies, including without limitation the university’s policies on outside activities and use of University trademarks and names. Further limits may be imposed.
Policy: Acceptable Use

upon personal use in accordance with normal supervisory procedures concerning the use of University equipment.

Network Infrastructure/Routing and Wireless Media

Users and units not authorized as Network Service Providers by the Chief Information Officer must not implement their own network infrastructure. This includes but is not limited to basic network devices such as hubs, switches, routers, network firewalls, and wireless access points. Users must not offer alternate methods of access to UFIT resources such as modems and virtual private networks (VPNs). Users must not offer network infrastructure services such as DHCP and DNS.

Authority:

UF-1.0102: Policies on Information Technology and Security

References:

Copyright Law of the United States: http://www.copyright.gov/

U. S. Trademark Law: https://www.uspto.gov/trademark/laws-regulations


U. S. Electronic Communications Privacy Act: https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285


UF Code of Student Conduct: https://sccr.dso.ufl.edu/students/student-conduct-code/

UF Sexual Harassment Policy: http://hr.ufl.edu/manager-resources/policies-2/sexual-harassment/
Policy: Acceptable Use

UF Electronic Mail Policy: https://it.ufl.edu/policies/email/electronic-mail/

Florida Statutes Chapter 119, Public Records:
http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0100-0199/0119/0119ContentsIndex.html