FLORIDA	OFFICIAL
POLYTECHNIC	UNIVERSITY
UNIVERSITY	POLICY

Subject/Title: Appropriate Use of IT Resources
FPU Policy Number: FPU-11.0018P
X New Policy __ Major Revision of Policy __ Minor Technical Revision of Policy
Date First Adopted: April 21, 2015
Date Revised:
Responsible Division/Department: Information Technology
Initiating Authority: Tom Hull, Vice President and CIO

A. APPLICABILITY/ACCOUNTABILITY:

This policy applies to all individuals who utilize, possess or have access to University IT Resources (a "User" as defined in Section C below).

B. POLICY STATEMENT:

1. User responsibilities. The University provides its IT Resources to authorized Users to facilitate the Users' legitimate objectives in a secure electronic environment. Each User is responsible for his/her use of any University IT Resources, including activity originating from the User's account within the User's control. Users are responsible for keeping their University accounts and passwords secure and may not share their University accounts or passwords with others.

   The use of University IT resources is a privilege and imposes certain responsibilities and obligations on Users whose use of University IT Resources is subject to state and federal law, as well as University regulations and policies (collectively referred to as "rules"). These rules apply when the User is accessing the Internet using University IT Resources and when using University mobile devices inside or outside the University premises. The rules include but are not limited to the following: the Student Code of Conduct (FPU-3.006) if the User is a student; the Personnel Code of Conduct and Ethics (FPU-6.002) if the User is an employee; the University's Sexual Harassment Policy (FPU1.005P); and state and federal laws and regulations governing the use of technology resources, including laws governing defamation, privacy, copyright, trademark, child pornography, the Florida Computer Crimes Act, the Electronic Communications Privacy Act, the Children's Online Privacy Protection Act ("COPPA"), and the Computer Fraud and Abuse Act.

2. User messaging. The User is responsible for practicing lawful, ethical and responsible messaging in a secure manner. All messages transmitted by a User through University networks and telecommunications systems must correctly identify the sender.

3. Limited expectation of privacy. Users should be aware that University IT Resources are not completely private and are subject to audits, the logging of activity, the monitoring of

general usage patterns and other such activities that are necessary to protect the integrity, security, or functionality of the University and the University IT Resources. The University employs passwords for the proper administration of its IT Resources only, and the requirement and use of a password should not give the User an expectation of privacy as to any information on a University IT Resource. A User has a limited expectation of privacy in the User's University email account, electronic data and communications on the University IT Resources.

All Users, including students, connecting their personal computers to the University network, are on notice that internal or external audits or other needs may require examination of uses of the University IT Resources or services and Users should not expect such uses to be free from inspection. The University network may be scanned for vulnerabilities, as a result, all Users, by connecting to the University network, acknowledge that network traffic to and from the User's computer may be scanned.

4. Monitoring of individual usage. Authorized University officers do not routinely monitor individual usage of the University computing Resources; however, the normal operation and maintenance of the University's IT Resources requires the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns and other such activities that are necessary for the provision of service. University officials may also specifically monitor the activity and accounts of individual Users of University IT Resources, including individual login sessions and the content of individual communications without notice to the User, when:
    a. The User has voluntarily made them accessible to the public.
    b. It appears reasonable and necessary to do so to protect the integrity, security, or functionality of University IT Resources or other computing resources, or to protect the University from liability.
    c. There is reasonable cause to believe that the User has violated or is violating this policy.
    d. An account appears to be engaged in unusual or unusually excessive activity; or
    e. It is otherwise required or permitted by law.

    Any such monitoring of communications, other than what is made accessible by the User, required by law, or necessary to respond to disruptions of network operations, must be authorized in advance by the appropriate Vice President in consultation with the Office of the General Counsel or the auditor.

5. Use must not disrupt. Users shall use the University IT Resources in a manner that does not disrupt other Users or damage the work of other Users. Users shall not use the University IT Resources in such a manner as to degrade or disrupt normal operations; to intentionally damage or disable the University network, telecommunications systems or computing devices; or to gain unauthorized access to anything.

6. Use for commercial purposes prohibited. University IT Resources shall not be used for non-University commercial purposes without the prior written approval of the University's CIO or designee.

7. Installation and use of software. Users may use only officially licensed software on University IT Resources. The use of the software must be consistent with the software licensing agreement and not copied or altered in violation of the software license. Users using University-owned mobile devices and tablets must obtain written permission from the University's CIO or designee to install software on those devices or tablets.

8. Use of copyrighted material. Copyrighted material may not be shared, copied or altered except as permitted by law.

9. Installation of network infrastructure. Users shall not install their own network infrastructure (including but not limited to the installation of hubs, switches, routers, network firewalls and wireless access points) on University premises. .

10. Audits conducted. The University conducts audits of the University network, telecommunications systems and IT Resources on a regular basis and on an as-needed basis.

11. No retaliation for reporting a security breach. The University will not retaliate against the individual(s) or entity reporting an observed or suspected security breach (the unauthorized access of data in an electronic form containing personal information).Individuals should report security breaches to the University Information Security Manager ("ISM") by calling (863) 874-8888 or sending an email marked "high priority" with the appropriate information to Helpdesk@FIPoly.org.

12. Policy violations. Examples of violations of this policy include but are not limited to:
    a. Attempting to obtain unauthorized access to computer systems or networks;
    b. Attempting to circumnavigate security procedures or obtain access to privileges to which the User is not entitled;
    c. Attempting to modify systems or software in an unauthorized manner;
    d. Transmitting mass messages without proper approval;
    e. Transmitting threatening or abusive messages in violation of University rules, regulations or policies, or the Student Code of Conduct;
    f. Releasing confidential, proprietary or protected information unless otherwise authorized or required by state or federal law;
    g. Illegal downloading of audio or video materials (including but not limited to movies, games and music) protected by copyright and not owned by the User; and
    h. Using personal "webcam" technology, including cameras on drones, to record video, audio or photos without permission where the other person(s) has a reasonable expectation of privacy such as in a dormitory room, locker room, treatment room, bathroom or University office, constitutes a violation of this policy. The Department of Public Safety and Police's use of cameras for security purposes is not prohibited by this policy.

13. Consequences of violating policy. Users found to have violated this policy are subject to disciplinary and other action, up to and including expulsion of the student or termination

of the employment of the employee or faculty member. In addition, the University may deny the violator access to University IT Resources. The University may also refer suspected violations of applicable law to the appropriate law enforcement agencies. Unauthorized distribution of copyrighted material, including unauthorized peer-to-peer file sharing, may subject the Users to civil and criminal liabilities.

14. Suspending, blocking or restricting User access. The University may suspend, block or restrict a User's access to IT Resources, independent of disciplinary procedures, when it reasonably appears necessary to do so in order to protect the University's resources.

15. The CIO or designee may grant exceptions to this policy as necessary for research and academic purposes on a case by case basis. Any such exceptions must be granted in writing.

C. DEFINITIONS:

1. **University IT Resources** means University computers, mobile computing devices, telecommunications systems, lab equipment, networks, printers, software, data, database systems and all other University-owned IT resources involved in the processing, storage, accessing and transmission of information.

2. **Users** means all individuals who utilize, possess or have access to University IT Resources whether through University IT Resources or through individual-owned bring your own devices ("BYOD") or computers accessing and transmitting information via University IT Resources.

POLICY APPROVAL

Academic Policy No.: FPU-11.0018P

Initiating Authority	Date 4/20/15
Policies & Procedures Committee Chair	Date 4-20-15
President/Designee	Date 4/21/15
Approved by FPU BOT, if required	Date