Policy Guidelines

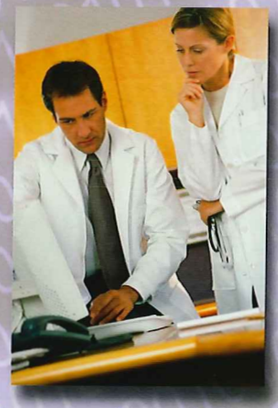
WHAT IS AT RISK?

- Productivity - The following have, potentially, a negative impact on our computer resources
  - unauthorized software
  - junk mail
  - websites featuring pornography, online gambling, dating, and game services
  - instant messaging (especially with file sharing)
  - downloading and storing pictures, video and music
- Reputation - The University's reputation is threatened when junk e-mail messages are sent or forwarded from UF e-mail accounts. The discovery of adult pornography on UF IT resources is damaging as well. So is downloading software that could permit a hacker to break into our network and steal data.
- Legal - Legal action can be taken against you personally if you use UF computing resources for
  - child pornography
  - spreading computer viruses or hoaxes
  - fraud
  - identity theft
  - illegal distribution of copyrighted material

UNIVERSITY OF FLORIDA HEALTH SCIENCE CENTER ACCEPTABLE USE POLICY CHECKLIST

As a good computing neighbor, I

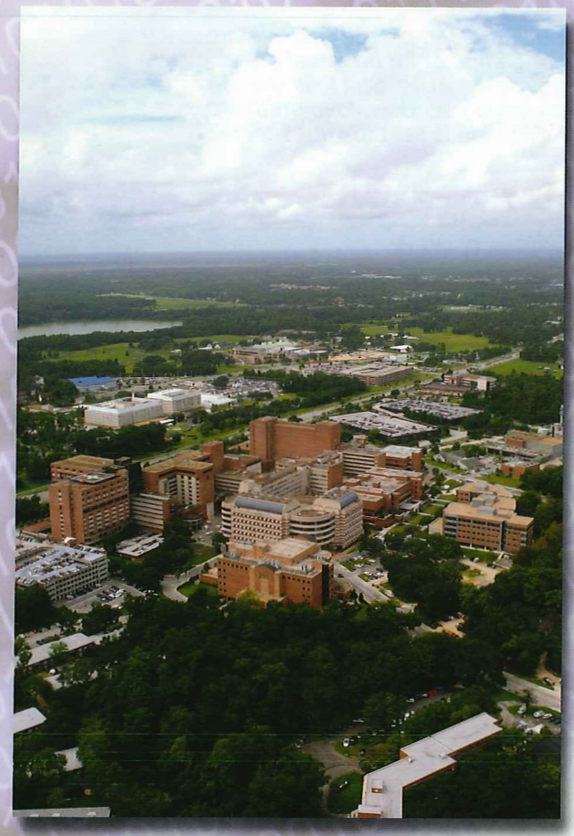
- ☐ Do not install software that my department hasn't approved
- ☐ Refrain from sending or forwarding junk e-mail or SPAM
- ☐ Visit web sites related to my work and check with my supervisor about visiting web sites for personal use
- ☐ Use safe and approved instant messaging software and avoid using it to send and receive files
- ☐ Download personal pictures, video and music to storage that only affects me (local drive on my workstation (if permitted), CD or a USB drive).



http://www.health.ufl.edu

UF | Health Science Center
UNIVERSITY of FLORIDA

UF | Health Science Center
UNIVERSITY of FLORIDA



Acceptable Use Policy (AUP) Guidelines for The University of Florida's Health Science Center (HSC)

HSC Acceptable Use

INTRODUCTION

The University of Florida (UF) acquires, develops, and maintains computers, computer systems and networks to facilitate direct and indirect support of UF's academic, research and service missions. The UF Acceptable Use Policy (AUP) combined with unit-specific policies and guidelines provide a framework describing acceptable and required behaviors involving Information Technology resources (IT-resources).

RATIONALE

Occasional personal use of UF IT-Resources is permitted when it

- is not for personal gain
- is not excessive or disruptive
- does not consume a significant amount of computing resources
- does not interfere with the performance of the user's job or other UF responsibilities and
- is otherwise in compliance with the UF AUP

Further limits may be imposed upon personal use in accordance with normal supervisory procedures concerning the use of UF equipment.

Be a good computing neighbor. Use your computer for work and check with your supervisor for personal uses.

Acceptable Use Policy: What Does It Mean To Me?

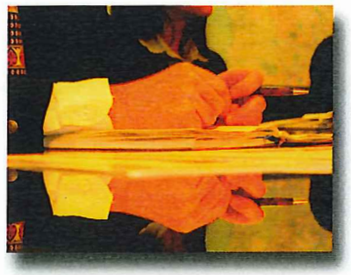
IT Resource: Defined. Any equipment that has the primary purpose to store, process, display, and/or transmit digital information in support of the missions of the University.

WHAT CAN I STORE?

Non-work related personal or licensed pictures, video, or music files consume large amounts of electronic storage. They should be stored on your local computer drive, or, better yet, on removable media like a USB drive or a CD ROM.

If these files are e-mailed to you, be sure to delete them. If you need to keep them, save them to a USB drive, a CD, or (if permitted) your computer's hard disk.

Beyond these examples you need to contact your supervisor to make sure the personal use is acceptable.



WHAT CAN HAPPEN TO ME?

- Your computer could break
- You could lose your work
- You could break other computers that share the network with yours (a very embarrasing situation)
- IT Staff may not be able to help you
- Your logon ID could be suspended
- You could face disciplinary actions
- You could face legal actions

SCENARIO

Embarrasing Situation. While trying to download pornographic files on your office computer you have a technical problem and call your IT support staff. The IT person encounters the pornographic files while trying to help you.

The IT support person first informs you that use of your computer for personal objectionable material is against the AUP. She tells she is not required to help you solve your download problem and walks away. Notification is sent to your supervisor.

WHEN CAN MY FILES BE ACCESSED BY SOMEONE BESIDES ME?

Routine IT Work

During the course of routine work (system performance monitoring, system audits, problem resolution, or security management) IT staff may encounter file or message content that you created. Your notice appears on a banner on your monitor before you logon to your UF computer.

While trouble-shooting your computer, IT staff may need to open a file or email message. You must be present or provide consent (verbal is fine) before they do so.

Business Related Emergencies

If you are unreachable and your supervisor needs email or content that you created, your Dean, Director or Department Chair may authorize access; however, you should expect to receive a notification from your supervisor.

Suspected Policy Violation or Legal Issue

If there is reasonable suspicion of a policy violation or a legal issue your files or email content may be accessed. It will be appropriately authorized by HSC Security, UF Privacy, HR or the General Counsel's Office depending upon the nature of the investigation. However, you should not expect to be notified.

SCENARIO

E-mail: Access by supervisor. *A supervisor asks IT staff for access to your e-mail because he suspects you are running a personal business from work.*

In order for a supervisor to access an employee's e-mail for a suspected policy violation such as in this scenario, they must have authorization from Human Resources and collaboration with the Office of General Counsel.

SCENARIO

File Access by Supervisor: You have a budget file stored in your "My Documents" folder that your supervisor needs. You are scuba diving in the Galapogos.

Your supervisor obtains permission from your Director, the IT staff gives your supervisor the file, and your supervisor sends you an email message notifying you of what took place.
PS. You should have given your supervisor this file before you went scuba diving.

HOW ARE VIOLATIONS PREVENTED?

Communication and technical controls are two approaches to help prevent violations of the Acceptable Use Policy.

- Good communication with your supervisor and manager of your IT department will help you understand the rules to be followed and the consequences if you do not.
- Technical controls approved by your unit leadership may be implemented. These are things such as:
  - quotas on the amount of e-mail you may store and the amount of files on network storage
  - blocking access to certain websites that can do damage to our computers
  - filters on file storage that limit the types of files you may store (*.mp3, *.jpg, *. wmv, etc.)

SCENARIO

Over-used Resource. During a routine scan of network storage, IT staff discovers that 63% of all department space is being consumed by your music flies.

IT staff may delete personal music files from shared HSC IT resources (networked drives) after providing good communication. IT staff will also remind you and your supervisor about the HSC AUP.

HOW IS THE AUP ENFORCED?

If you violate the AUP, you and your supervisor will be notified. The notification will include helpful information that describes the violation and suggests steps for its remedy. After this notification you and your supervisor

- will agree on a time frame for getting the violation in check
- determine and execute steps to prevent the violation in the future
- will re-read the AUP Guide

SCENARIO

Visiting game web sites: Computer virus. A virus has to be removed from your computer. IT staff told you it came from a game web site you visited.

You and your supervisor are notified. You agree not to do it again.

WHAT HAPPENS IF I DON'T COMPLY?

If you continue to violate the AUP or if the violation goes unaddressed, you will be warned that your account may be suspended.

If your account is suspended it can only be re-activated upon assurance from you and your supervisor that the unacceptable use will stop.

Supervisors should use judgment to determine whether disciplinary action is necessary. If this is the case, then Human Resources must be involved.

SCENARIO

Visiting game web sites: Computer virus. IT staff has cleaned a virus off of your computer for the third time. You didn't tell them you were still visiting game web sites because you were afraid they would suspend your account as forewarned.

It doesn't matter that you didn't tell IT staff. Since this is a repeat violation of the AUP and you and your supervisor were warned about account suspension, your account will indeed be suspended. Your account can be re-activated after you and your supervisor provide assurance that the activity will not happen again. Your behavior may result in additional disciplinary action involving HR.