Information and Communications Technology (ICT) Policy

This policy applies to all clients of ICT resources and ICT equipment owned, leased, or rented by the University of ISU. It also applies to any person connecting personal equipment to the University network from any location. This includes, but is not limited to:

- All students,
- Academic, visiting academic and non-academic staff,
- Guests of University staff, and
- External individuals or Organisations.

ICT equipment includes, but is not limited to:

- Wireless access cards, network interfaces and dialup modems.
- Desktop, notebook, mobile devices and personal digital equipment.
- Peripheral devices such as printers, scanners.
- Servers.
- Networking equipment and communications networks used to link these components together and to the Internet.

As a condition of using the University of ISU's ICT resources, you agree that you will comply with all copyright and other intellectual property laws and agreements.

You also agree that in using the system you will not violate any civil or criminal laws.

Furthermore, you agree to indemnify and protect the University (and its representatives) from any claim, damage, or cost related to your use of the University's ICT resources.

Use of ICT facilities is at all times subject to the conditions and constraints relating to their use in terms of University security, privacy, copyright, confidentiality policies, standards, and guidelines.

Unauthorized Use

- You agree not to share passwords that are provided for access to University services.
- You agree not to use a computer account that does not belong to you.
- You agree to refrain from any activity that intentionally interferes with a computer's operating system or its logging and security systems, or that may cause such effects.
- You shall be sensitive to the public nature of computer systems and refrain from transmitting, posting, or otherwise displaying material that is threatening, obscene, discriminating, harassing or defamatory.
- You agree not to make copies of, or distribute, software the University owns or uses under license, unless permission to copy has been specifically granted by the owner of the software or the owner of the license. If in doubt as to whether you have permission to copy software, assume you don't.
- You agree not to create, alter, or delete any electronic information contained in any system associated with University ICT resources that is not part of your own work.
- You shall not use University of ISU's ICT resources as a means of obtaining unauthorized access to any other computing systems.

You agree not to intentionally access, download, store, or distribute material of a pornographic nature other than with the approval from an authorized University Officer for research related purposes.

- You agree not to perform any monitoring, scanning or “sniffing” of the University ICT network unless authorized by the Manager Information Technology Services.

Unauthorized Personal Use

Unauthorized use of Information Communication Technology includes, but is not limited to:

- Infringing the copyright or other intellectual property right of the University or third parties
- Scanning and/or printing resources protected by copyright
- Disrupting communication and information devices through such means as mass emailing or transmitting files which place an unnecessary burden on University resources.
- Disrupting or interfering with the use of Information Communication Technology
- Effecting security breaches of network communication – security breaches include, but are not limited to, accessing data of which the client is not an intended recipient, and logging in to a server or account that the client is not authorized to access
- Executing any form of unauthorized network monitoring
- Circumventing user authentication or security of any host, network, or account
- Without authority: destroying, altering, dismantling, disfiguring, preventing rightful access to, or otherwise interfering with, the integrity of Information Communication Technology
- Accessing offensive internet sites.
- Storing of non-academic related material in the network drive share allocated.

Users may not use internet or email access to:

- Download, distribute, store or display pornographic and other offensive graphics, images or statements, or other material obtained from offensive internet sites
- Download, distribute, store or display material that could cause offence to others (for example, offensive material based on sex, gender, ethnicity or religious and political beliefs)
- Download and store illegal music, videos and software.
- Download large amounts of material for personal use
- Download information for external Organisations or the general public, without Authorisation
- Distribute chain letters
- Distribute defamatory, obscene, offensive, or harassing messages
- Distribute confidential information without authority
- Distribute private or personal information about other people without Authorisation
- Distribute messages anonymously, using a false identity, or using another person’s user or email details.

Malware (Virus and Spyware)

- Scan any removable media (USB flash drives, External hard-disks etc.) prior to using them or copying any program files contained on removable media to the University computers.
- Electronic mail messages and Internet file transfers may contain files that could potentially carry malware. Scan these files prior to using them on the computer.

If your computer is infected or suspect that your computer may be infected by malware, contact the ICT Services helpdesk immediately so that measures can be taken to remove the malware and identify any other affected computers and storage media.

Violations

Any suspected violations should be reported to the ICT Services office immediately.

Violation of this policy may result in fines and suspension of your ICT services and may also lead to disciplinary actions by the University.

Fines

The following Fines apply to those violating ICT Services Regulations.

1. Breaking computer lab regulations and policies:–

- **First offence – $10-00 and user accounts disabled until fine is paid.**
- **Second Offence – $20-00 and user accounts disabled until fine is paid.**
- **Third Offence – $30-00 and user accounts disabled for 4 weeks.**

2. Password reset $0.50 per request. (Password resets done during enrolment is free)