University Policies

Acceptable Use of Technology Policy

Policy Statement

Use of East Stroudsburg University (ESU) information technology resources is a privilege and signifies agreement to comply with this policy. Users are expected to act responsibly and follow the policies and any applicable laws related to the use of information technology resources.

This policy applies to all faculty, staff, students, contractors, temporary personnel, vendors and visitors.

The university reserves the right to limit, restrict, or extend information technology privileges.

Information Technology resources are intended to support the university's instructional, research and administrative operations

While ESU recognized the role of privacy in institutions of higher learning and will endeavor to honor that ideal, there is no expectation of privacy of information stored on or sent through the University's resources, except as required by law.

POLICY HISTORY

Policy Number:
ESU-2012-01-A

Policy Number History:
Formerly ESU-FA-2011-032-A

Effective:

Adopted:
April 11, 2012

Last Reviewed:
November 18, 2016; April 2, 2018

Amended:
February 14, 2017; April 2, 2018

Related Policies:
Wireless Communications Stipend, Discrimination & Harassment, Protection of Minors, Sexual Harassment, Sexual Harassment & Title IX Compliance

Acceptable Use Policy Defined

An acceptable use of information technology policy defines the capabilities and limitations of the use of information technology resources to insure that resources are available to all approved users and that the use of information technology complies with state and federal laws.

Information technology resources include, but are not limited to, university owned or operated hardware, software, computing equipment, systems, networks, programs, personal data assistants, cellular phones, fax, telephone, storage devices, cable television, security cameras, input/output, connective devices via either a physical or wireless connection regardless of the ownership of the device connected to the network, and any electronic device issued by the university.

Privacy

Users should have no expectation of privacy of information stored on or sent through the university-owned information technology resources, except as required by law.

Data Network Connectivity (Hard-Wired Connection)

All equipment, devices and computers connected to the data network are the responsibility of the university's Computing and Communication Services. Computing and Communication Services reserves the right, at its discretion, to limit, restrict or terminate the use of equipment or services, unauthorized or authorized, that Computing and Communication Services perceives to be an impediment or compromise to its ability to securely deliver the services for which it is responsible. Any devise that needs to connect to the data network must be authorized and configured by Computing and Communication Services. Personally owned equipment, except for equipment owned by residence hall students, is not permitted to connect to the data network without written permission from Computing Services.

Wireless Network Connectivity

A wireless network, where available, is provided as a convenience to any ESU authorized user. Personally owned devices may connect to the wireless network and, upon doing so, are subject to this acceptable use policy. Technology connecting to the wireless network is subject to a security scan to protect technology resources.

Telephone Use (including FAX)

The university recognizes there may be occasional times when personal calls must be made or received during business hours. Such calls are to be held to a minimum and must not interfere with the employee's work. When a long distance charge is required for a personal call the call must be billed to the caller's home phone number or the charge must be reimbursed to the university.

Responsible Use of Technology

1. Respect the intellectual property rights of authors, contributors and publishers in all media.
2. Protect user identification, password, information and systems from unauthorized use.
3. Report lost or stolen devices immediately upon loss.
4. Use technology in compliance of state and federal laws.
5. Adhere to the terms of software licenses.
6. Notify Computing and Communication Services of possible misuse of technology or potential security holes.

Prohibited Use of Technology

1. Use of information technology resources to display, hold, send, view, print, download, retransmit, distribute or otherwise communicate content which the University may deem to be indecent, obscene, sexually explicit, or pornographic is prohibited absent a legitimate academic or research purpose.
2. Use of information technology resources by anyone to display, hold, send, view, print, download, retransmit, distribute or otherwise communicate child pornography is illegal and therefore strictly prohibited. Any occurrence of child pornography material is a violation of federal and state statutes and must be immediately reported to University Police as required by law and University policy.
3. Use of information technology resources by anyone to send threatening or harassing content or messages or to view, download, retransmit, distribute, or otherwise communicate content or messages that may violate the University's policy on Discrimination & Harassment and/or policy on Sexual Harassment and Title IX, is prohibited. Electronic threats and harassment are taken as seriously as any other threats or harassing behavior or communication.
    - Anyone who receives a threatening communication should immediately bring it to the attention of University police.
    - Anyone who receives a sexually harassing communication should immediately contact the Office of Employee Relations or Title IX Coordinator.
    - Anyone who receives a communication that harasses on the basis of any protected classification, including race or national origin, should immediately contact the Office of Employee Relations or Campus Life and Inclusive Excellence.
4. Providing false or misleading information to obtain or use university technology resources.

5. Use of information technology resources for personal financial gain or a personal commercial purpose.
6. Use of information resources are not to be used in support of or for illegal activities.
7. Unauthorized use of another user's account or attempting to gain access to another user's account.
8. Sharing of accounts.
9. Interfering with the normal operation, proper functioning, security mechanisms or integrity of technology resources.
10. Use of technology resources to transmit abusive, threatening or harassing material, chain letters, spam, phishing scams or other communications prohibited by law.
11. Copyright infringement including, but not limited to, illegal sharing of video, audio, software or data.
12. Excessive use that overburdens the technology resources. Computing Services reserves the right to set limits on excessive use.
13. Installing a server or running server software without written permission from Computing Services.
14. Intentionally or knowingly installing or executing a program or file that could result in damage to university technology.

Compliance

Failure to comply with this policy may put University information assets at risk and may have disciplinary consequences for employees and University affiliated organization members, up to and including termination of employment (see item "c" of appeal statement below.) Students who fail to adhere to this policy may be referred to the Student Conduct & Community Standards Office. Contractors and vendors who fail to adhere to this policy may face termination of their business relations.

Reason for Policy

The acceptable use of information technology policy defines the capabilities and limitations of the use of information technology resources to ensure that these resources are available to all approved users and that the use of information technology complies with state and federal laws.

Appeal Statement

Those individuals who are found in violation of the policy may submit a written statement of appeal to one of the following:

1. Students can appeal to the Vice President of Campus Life and Inclusive Excellence;
2. Staff can appeal to their Supervisor or next-level manager; or
3. Any bargaining-unit member of any Union with membership on campus maintains their contractual and respective grievance rights, should disciplinary action be taken for a violation of this policy. No appeal of any disciplinary action will occur outside of the afforded contractual grievance process.

This appeal must be in written form and submitted to the respective party within 10 academic days of receiving the disciplinary action. The appeal process can take up to 30 academic days at which time the determining party's decision is final.

Definitions

Information Technology Resources: includes, but is not limited to, all university owned, operated, or contracted for hardware, software computing equipment, systems, networks, program, cellular phones, smartphones, fax, telephone, storage devices, cable television, input/output, connecting devices via either a physical or wireless connecting devices via either physical or wireless connection regardless of the ownership of the devise connected to the network, and any electronic device issued by the University. The acceptable use policy must be followed by university employees, students, contractors, and guests.

Other Relevant Information

☑ Acceptable Use of Technology Procedures

EXPLORE MORE

University Policies

List of Policies

Policy User Resources

Policy Owner Resources

The Office of the President should be contacted with questions concerning this website or the policies listed on it.

CONTACT INFORMATION

Reibman Administration Building
(570) 422-3545
(570) 422-3478 (Fax)

Policy Development Specialist