

Policies and Procedures



Use of ESF Computing and Network Resources

Introduction:

The electronic resources of the State University of New York College of Environmental Science and Forestry (ESF) are powerful tools, shared among members of the campus community, designed to support and benefit the teaching, research, public service, administrative and other activities of the College. Computing and network resources are defined as including, but not limited to, hardware, software, e-mail, peripherals, electronic files in text, image and audio form, Internet access, and web pages. Individuals using these resources are expected to do so wisely and carefully, with respect and consideration of the rights, needs and privacy of others. The preservation of this privilege for the full community requires that each faculty member, staff member, student, and other authorized user comply with institutional and external standards for appropriate use. This is not a comprehensive document covering all aspects of responsible use, but rather is meant to outline general principles and responsibilities.

This policy supplements all applicable SUNY and College policies, including sexual harassment, patent and copyright, and student and employee discipline, as well as applicable federal and state laws.

General Principles:

1. This policy applies to all ESF computing and network resources, including host computer systems, ESF-sponsored computers and workstations, software, data sets, and communications networks controlled, administered, or accessed directly or indirectly by College resources, employees, or students.
2. Authorized use of computing and network resources owned or operated by ESF or for the benefit of the College via the Research Foundation of SUNY shall be consistent with the education, research and public service mission of the College and consistent with this policy.
3. Authorized users of ESF computing and network resources include currently employed faculty and staff, currently enrolled students, and other affiliated individuals or organizations authorized by the President or his designee. Use by non-affiliated institutions and organizations shall be in accordance with SUNY Administrative Procedures Man-

ual Policy 007.1: Use of Computer Equipment or Services by Non-affiliated Institutions and Organizations.

4. ESF reserves the right, upon reasonable cause for suspicion, to access all aspects of its computing systems and networks, including individual login sessions, to determine if a user is violating this policy or state or federal laws.
5. ESF reserves the right to limit access to its networks when applicable campus or university policies or codes, contractual obligations, or state or federal laws are violated, but does not monitor or generally restrict the content of material transported across those networks.
6. ESF reserves the right to remove or limit access to material posted on university-owned computers (or privately owned computers connecting to the ESF campus network) when applicable campus or university policies or codes, contractual obligations, or state or federal laws are violated, but does not monitor the content of material posted on university-owned computers.
7. ESF reserves the right of individual supervisors to direct the removal from College equipment of any non-College related screensavers, wallpaper, or music.
8. Remote access to ESF resources shall not compromise the security of the ESF network. If security is compromised, individual access may be denied or revoked.
9. Users must register with Computing and Network Services (CNS) if they wish to connect a computer to the network.
10. Reasonable precautions should be taken to prevent theft of ESF computers and compromising ESF information residing in electronic format.

User Responsibilities:

Privacy: No user should view, copy, alter or destroy another's personal electronic files without permission (unless authorized by the ESF College administration or required to do so by law or regulation) of the owner of the files. Users shall not intentionally seek information on, obtain copies of, or modify files or passwords belonging to others.

Copyright: Written permission from the copyright holder is required to duplicate any copyrighted material. This includes duplication of audiotapes, music, videotapes, photographs, illustrations, computer software, and all other information for educational use or any other purpose. Most software that resides on ESF computing network(s) is owned by the College, or third parties, and is protected by copyright and other laws, together with licenses and other contractual agreements. Users are required to respect and abide by the terms and conditions of software use and redistribution licenses. Such restrictions may include prohibitions against copying programs or data for use on ESF computing network(s) or for distribution outside the College; against the resale of data or programs, or the use of them for non-educational pur-

poses or for financial gain; and against public disclosure of information about programs (e.g., source code) without the owner's authorization.

Title II of the Digital Millennium Copyright Act: This Act limits the liability of an Internet service provider (ISP) for certain copyright infringements. One definition of an ISP is “a provider of online services or network access, or the operator of facilities therefore.” ESF can be considered an ISP for students, faculty and staff and is eligible for the limitations on liability. More information regarding this act can be found at <http://webinfo.esf.edu/administration/dema.htm>.

Harassment, libel and slander: Under no circumstances, may any user use ESF computing and network resources to libel, slander, or harass any other person.

Access to Computing Resources:

- **User accounts:** Accounts created by an ESF CNS administrator for an individual are for the use of that individual only. Users must use ESF passwords and account ID's to access any services on the network.
- **Sharing of access:** Computer accounts, passwords, and other types of authorization are assigned to individual users and should not be shared with others. The holder of the account is responsible for any use of that account. Account holders may authorize designees to use the account for College purposes. If an account is shared or the password is divulged to any person not appropriately acting as a designee of the account holder, the holder of the account may lose all account privileges and be held responsible for any actions that arise from the misuse of the account.
- **Permitting unauthorized access:** A user may not run or otherwise configure software or hardware to intentionally allow access by unauthorized users.
- **Termination of access:** When an employee is no longer a member of the campus community (e.g., withdraws, graduates, retires, terminates employment, or otherwise leaves the College) or is assigned a new position and/or responsibilities within the College, access authorization must be reviewed and access may be terminated. Individuals must not use computer facilities, accounts, access codes, privileges or information for which they are not authorized in their new circumstances.
- **Virtual private networks:** Any connection between firewalls over public networks must use encrypted Virtual Private Networks (VPN's) to ensure the privacy of the data passing over the public network. CNS must approve all VPN connections prior to implementation.
- **Wireless networks:** CNS must approve all wireless networks or access points before they are installed.

Circumventing security: Users are prohibited from attempting to circumvent or subvert any College system's security measures. Users are prohibited from using any computer program or device to intercept or decode passwords or similar access control information.

Breaching security: Deliberate attempts to degrade the performance of a computer system or network or to deprive authorized personnel of resources or access to any ESF computer or network is prohibited. Breach of security includes, but is not limited to, the following: creating or propagating viruses, hacking, password grabbing, and disk scavenging.

Abuse of computer resources: Abuse of ESF's computer resources is prohibited. Users are expected to use College computing resources in a responsible manner consistent with the instructional, research, and administrative goals of the College. Users are expected to refrain from engaging in deliberate wasteful practices. Abuse includes, but is not limited to, the following:

- **Game playing:** Recreational game playing in a public computing facility is prohibited.
- **Unauthorized monitoring:** A user may not use computing resources for unauthorized monitoring of electronic communications.
- **Excess use of resources:** Users are prohibited from using or authorizing others to use excess resources such as network bandwidth or disk storage. Users shall not download large files such as graphic, streaming media and audio files unless they are directly related to the user's job function or other College purposes.
- **Pornographic material:** Users may not intentionally access or download any kind of pornographic material. Any such material that is received should be deleted immediately.
- **Unauthorized use of software:** All users are responsible for ensuring the legal use of their software.
- **Unauthorized servers:** Initiating and operating unauthorized servers (FTP, file sharing applications, e-mail, etc.) on ESF servers or systems, including those that extend ESF network and computing resources to non-affiliates of the College, is prohibited unless prior approval is given by the Director of Information Technology. CNS has oversight responsibilities for all servers on the ESF network. CNS reserves the right to shut down servers that are unauthorized, running unauthorized server programs, or interfering with the ESF network.
- **Use of an alias:** A user may not develop programs or use any mechanisms to alter or avoid accounting for the use of computing services or to employ means by which the facilities and systems are used anonymously or via an alias.
- **Private commercial purposes:** The computing resources of ESF shall not be used for personal or private commercial purposes or for financial gain.

- Political advertising or campaigning: The use of ESF computers and networks for political advertising or campaigning is prohibited.

Limitations on Users' Rights:

1. The issuance of a password or other means of access is to assure appropriate confidentiality of ESF files and information and does not guarantee privacy for personal or improper use of university equipment or facilities.
2. ESF provides reasonable security against intrusion and damage to files stored on the central facilities. ESF also provides some facilities for archiving and retrieving files specified by users and for recovering files after accidental loss of data. However, the College is not responsible for unauthorized access by other users or for loss due to power failure, fire, floods, etc. ESF makes no warranties with respect to Internet services. ESF specifically assumes no responsibilities for the content of any advice or information received by a user through the use of ESF's computer network.
3. Users should be aware that ESF's computer systems and networks might be subject to unauthorized access or tampering. In addition, computer records, including e-mail, are considered "records" which may be accessible to the public under the provisions of the New York State Freedom of Information Law or pursuant to discovery in a legal proceeding.

Sub-domains

Sub-domains or child domains may be created for various ESF departments, office or research entities. In each case, information ownership will be delegated to an individual(s) within the specified area. Information owners are responsible for determining who should have access to protected resources within their jurisdiction and determining specific access privileges for individuals. Responsibility for implementing security measures may be delegated, though accountability remains with the information owners. Network controls must be developed, implemented by the sub-domain owners and then reviewed by CNS to ensure that an authorized user can access only those network resources and services necessary to perform his or her job responsibilities.

Incidental Personal Use of Information Technology:

Incidental personal use of computing resources at ESF is an exception to the general prohibition against the use of College equipment for anything other than official state business and educational activities. The parameters of the exception are:

1. The incidental personal use of computing resources facilitates the user's proficiency; and
2. There is no additional cost to the state.

Incidental personal use must not:

1. Result in personal financial gain for the user;

2. Conflict with performance of assigned job responsibilities;
3. Be in violation of existing security/access rules; or
4. Violate this or other College policies or applicable federal or state laws.

Violations:

It is the responsibility of all users of the campus computing resources and network to notify CNS about violations of laws and College policies in connection with the use of the computing resources and network, as well as about potential weaknesses or threats to security of the ESF campus network. The user community is expected to cooperate with CNS in its operation of these resources, as well as in the investigation of system misuse or abuse. Any concerns, complaints, or reports of misconduct with regard to the ESF e-mail system or campus network should be reported to the Director of Information Technology and Institutional Planning at 470-6621 or the Director of Administrative Computing at 470-6689.

Sanctions:

ESF Administration reserves the right to deny, limit, or revoke computing and network privileges at its discretion. Alleged violations of this policy or violation of other College policies in the course of using the computing resources and network may result in an immediate suspension of campus network privileges and may also result in the referral of the matter to ESF Administration, University Police, or other appropriate authority for action. Violators of this policy will be subject to the existing student or employee disciplinary procedures of ESF. Illegal acts involving ESF computing resources may also subject users to prosecution by state and federal authorities.