Introduction

• The following training materials will reference the contents of the Computer Use Regulations, but should not serve as a substitute for reading the actual regulations. This training is meant to serve as an introduction to and notification of the general responsibilities NCSU employees have under the regulations.

• North Carolina State University's computer networks, equipment and resources are owned by the University and are provided primarily to support academic and administrative functions. Their use is governed by federal law, state law, and University policies and procedures.
As members of the Office of Information Technology we are entrusted with a high level of responsibility, control of, and access to University information resources and infrastructure.

As privileged users and administrators we must set the ethical and professional standards for NC State.
Policies

There are seven additional policies / regulations directly related to computer use at NCSU and this training will touch on aspects of all of them. For complete information though you should refer directly to the following at: http://www.ncsu.edu/policies/informationtechnology

- Computer Use Policy (POL08.00.1)
- Computer Use Regulation (REG08.00.2)
- Software Licensing Requirements (REG08.00.8)
- Data Management Procedures (REG08.00.3)
- Copyright Infringement Policy Statement (REG01.25.2)
- Home Use of Equipment (REG07.30.14)
- University Record Retention and Disposition (REG01.25.12)
Additional References

- Advice Memo on Public Computers and Pornography: [http://www.ncsu.edu/policies/informationtechnology](http://www.ncsu.edu/policies/informationtechnology)
- Copyright information: [http://www.ncsu.edu/copyright/](http://www.ncsu.edu/copyright/)
- Safe Computing at NC State [http://oit.ncsu.edu/safe-computing](http://oit.ncsu.edu/safe-computing)
- Peer-to-peer (P2P) file-sharing [http://oit.ncsu.edu/p2p](http://oit.ncsu.edu/p2p)

**Contact Info:** DMCA copyright agent - John Baines, Assistant Director, Security and Compliance Unit. JOHN_BAINES@NCSU.EDU, 513-7482
Pornography
Pornography

There are several ways in which pornography creates conflicts in the NC State computing environment.

CONFLICT 1

• Sensitive subject for state legislators & auditors – most state agencies ban it outright
• Yet, university shared computers are bound by free speech requirements

CONFLICT 2

• University prizes constitutionally-protected free speech
• Yet, must not allow sexual harassment situations to occur
Pornography

Pornography loses its constitutional protection in three situations:

- Child pornography (criminal offense to possess or distribute – this includes accessing it by computer)
- Obscenity (criminal offense to distribute)
- Sexual harassment (civil liability under non-discrimination laws)
Regulatory Limitations
Regulatory Limitations

User Accounts
University employees should not share their accounts with anyone.

- Meaning they should not let someone else use a computer or resource that they’ve signed into, or share their username and password with someone else so that they may use University resources.

- Employees should also not set up an automated way to share their access with other users via web proxy, anonymous remailer, or other means.
Regulatory Limitations

Guest Accounts

Users should not share their access with anyone regardless of how short a time that guest requires access, and regardless of whether the access request is legitimate.

Rather they should request a guest account through proper channels.
Regulatory Limitations

**Guest Accounts cont.**

Departments may establish guest & temporary accounts for authorized use of University IT Resources by non-university personnel.

The responsible department must ensure the Computer Use Policy and Regulations are understood and adhered to by the users of the accounts. The users of the accounts are responsible for adhering to University regulations and all state and federal laws.
Regulatory Limitations

Federal & State Laws

“Use of University computing systems and networks must comply with federal and state law.”

State Policies

“Use of University computing systems and networks must not violate any policy or directive of the Board of Governors, the NC State Board of Trustees, the UNC General Administration, or the NC State administration.”
Regulatory Limitations

Email / Network Data

The University may examine personal electronic information stored on or passing over University equipment or networks to:

• “Insure the security and operating performance of its systems and networks.”
• Conduct an audit.
• Investigate an issue before bringing it to the University Institutional Review Board.
• Comply with E-discovery rules connected to a subpoena or other court document.
• “Enforce University policies or compliance with state or federal law where examination is approved in advance by a dean, vice chancellor, or vice provost, and:
  • “There is suspicion a law or University policy was violated, or”
  • “Examination is necessary to comply with a state or federal law.”
Continued...

Computer Users should have no expectation of privacy in personal material stored by them on the University computing systems when:

- There is a reasonable suspicion that a law or University policy has been violated, or
- “Examination is necessary to comply with a state or federal law.”

If there is information you wish to keep private and personal you should not store it on University equipment.

At the very least personal information should be stored in a separate folder and labeled as “personal”.

University IT staff are in a very privileged position when it comes to access to data, so they should always bear both legal and cultural requirements for privacy of the individual firmly in mind when accessing any university data.
Regulatory Limitations

Confidential Passwords

Although the University may authorize confidential passwords, or other secure authentication / encryption, this does not imply the information accessed or sent with them over the University systems or networks is private. While general content review will not be undertaken, monitoring of this material may occur for the reasons specified (previously).

If there is information you wish to keep private and personal you should not send it using your University email or over the University network regardless of whether your authentication / encryption method is confidential.
Regulatory Limitations

Work-Related Access to Business Information

A supervisor or other university official may have work-related access to information stored on University computing systems without permission or approval.

If personal and business information are not clearly separated, they may examine all information to the extent needed to separate and access business information for work-related purposes.
Active Monitoring

University IT security staff may use low risk scanning of computers and monitoring of network traffic to detect compromised machines and to identify vulnerable services. The IT security staff will report these discovered incidents to appropriate users wherever possible and in a timely manner.
Regulatory Limitations

Log Monitoring

University IT security personnel will need access from time to time to individual computer log information for operational or business purposes. These logs may contain sensitive information about the identity of the users and the Internet sites they have been visiting as well as the identity of those whom they have been communicating with. Again, legal and cultural requirements for individual privacy will be respected as far as possible.
Limits on Access & Storage

- Deans or Vice Chancellors may approve rules to exclude personal files from storage on network drives, in which case all files and data on the affected systems may be treated as information related to University business.

- “The University reserves the right to limit or revoke access to University computing systems or networks when:
  
  - Federal laws, state laws, or University policies are violated, or
  
  - Where University contractual obligations or University operations may be impeded.”

- Attempts will be made to notify affected users.
Sender Identification

“All material prepared and utilized for purposes of University business and posted to or sent over University computing equipment, systems or networks must:”

 Ramirez

¢ Accurately and correctly identify the sender, unless a University administrator (department head or higher) approves anonymity for a University business purpose.

¢ Be limited to information needed for University business.

“Any traffic on the University’s networks may be monitored for operational or research purposes.”
Regulatory Limitations

Sender Identification continued
University IT security personnel will need access from time to time to individual computer log information for operational or business purposes.

These logs may contain sensitive information about the identity of the users and the Internet sites they have been visiting as well as the identity of those whom they have been communicating with.

Again, legal and cultural requirements for individual privacy will be respected as far as possible.
Continued...

“No one who is conducting University business using University computing resources may convey personal statements that could be construed as representing the positions or beliefs of the University.”

Personal statements are not allowed in signature blocks; signatures should not include:

- Religious views
- Political campaign positions
- Proselytizing remarks
- Quotations
Computer Registration

University computers must be registered with NC State in the ncsu.edu domain.

It is forbidden to register a non ncsu.edu domain for any computer connected to the NC State network without prior approval; there are few exceptions.

Owners of approved non-ncsu.edu domains must make it clear that they are using computing and networking resources belonging to NC State for delivery.
Regulatory Limitations

Software

Software will be used only in accordance with its license agreement.

All software use must be within the terms of the license agreement (e.g., number of users, computers, data volumes, etc.).

Software piracy will not be condoned by the university.

Unless otherwise provided in the license, any duplication of copyrighted software, except for backup or archival purposes may be a violation of copyright law.
Regulatory Limitations

Security Precautions

Users of IT resources must take appropriate security precautions in order to prevent computer infection, mis-use or data leakage.

These precautions include:

- Ensuring critical vendor-supplied security patches are applied to software products in a timely manner
- Following the university Antivirus Software Requirements regulation and
- Following the university Administrative Password Standard.
Personal Use
Personal Use

Limits of Personal Use for Authorized Users

“Authorized users may access University computing equipment, systems and networks for personal uses if the following conditions are met:

- There is no expectation of privacy
- Does not overload the University computing equipment or systems, or negatively impact the system's performance.
- Does not result in commercial gain or private profit, except as allowed under University intellectual property policies and the external activities for pay policy.
- In no case may University computing resources be used for solicitation of external activity for pay
- Does not violate any laws, University policies on copyright and trademark, or licensing agreements.
Personal Use

Limits of Personal Use for Authorized Users, cont.

- Does not state or imply University sponsorship or endorsement.
- Does not violate any law or University policy, regulation, or rule, including the Equal Opportunity and Non-Discrimination Policy Statement.
- The use does not involve unauthorized passwords or the abuse of identifying data and/or tools that attempt to circumvent system security or that in any way attempt to gain unauthorized access.
- This constitutes a "no criminal hacking" standard for approved use of university IT resources.
Personal Use

Limits of Personal Use for Authorized Users, cont.

* Does not involve sending or soliciting chain letters, or sending unsolicited bulk mail messages (e.g., "junk mail", "spam", or “MLM”).
* Does not result in any direct cost to the University.
* Must be done on an employee's own time, not during hours when they are being paid to work.

“Any creation of a personal World Wide Web page or a personal collection of electronic material that is accessible to others must include a disclaimer that reads as follows:

"The material located at this site is not endorsed, sponsored or provided by or on behalf of North Carolina State University."
Copyright

What is copyright?
Copyright is a legal right to control the copying, distribution, modification, display, and performance of certain types of works. It applies to text, graphics, video, audio, and many other forms of expression.

How can I use copyrighted material?
In general, you must have permission from the copyright holder to copy, distribute, modify, display or perform their work. There are few legal ways you can use copyrighted material in these ways without first obtaining permission from the copyright holder.
Copyright

Infringement complaints about using copyrighted material for official NC State business
NC State University has the twin objectives of minimizing liability while also providing legal
support for the activities of faculty and staff.

Infringement complaints regarding personal use of copyrighted materials
The university follows official takedown and notification procedures as established by federal
law.

What are NC State's policies regarding electronic copyright infringement?
NC State will terminate the computer accounts of repeat infringers. Other disciplinary actions
may also be taken.
Copyright

Digital Millennium Copyright Act

DMCA - Copyright violation complaints must be reported to the designated university agent.

Industry-specific groups concerned with Internet anti-piracy include:

- RIAA
- Film studios - MPAA
- Business Software Alliance etc.

- The University follows up on all notifications of suspected copyright violation
- Individuals may be subject to legal action from the copyright holder.

From security incident info reported to SBI
File Sharing
What is File Sharing?

- File sharing is the act of making files on one computer accessible to others on a network. There are many legitimate uses of file sharing. Lately peer-to-peer (P2P) file sharing has brought about significant exposures, however.

- P2P file sharing causes every individual computer running the P2P software to act as a server to every other computer on the P2P network across the Internet.
File Sharing

Continued...

• This can cause shortage of disk space, overloaded processors, network denial of service situations and many other performance problems.

• Also, it often involves the sharing of copy-written material such as music, movies, TV programs, games and software.

By using most P2P file sharing programs, by default you make all data on your computer available to unauthorized users on the P2P network, including your personal information, confidential university business data and your personally licensed copyright material.
File Sharing

What are some popular File Sharing applications?
Just like computer viruses, there are more file sharing applications being created every day, but here is a list of some common ones:

- BitTorrent
- Limewire
- Kazaa
- Gnutella

⚠️ Remember, the software used for file sharing itself is not illegal, it is the downloading or sharing of copyrighted material using this software that is the illegal action.

- Paying for a file sharing application does not mean you have paid for subsequent downloads.
- There are many legitimate uses of file sharing software and so NC State does not restrict network activities that make use of this type of software.
File Sharing

What happens if I’m caught doing illegal File Sharing at work?
“Misuse of state property or funds may result in disciplinary action up to and including dismissal.”

Why is File Sharing illegal?

File Sharing is not necessarily illegal, depending on the nature of the files being shared, it is a legitimate technology, which is sometimes used for illegal purposes.

It becomes a legal issue when the person sharing the files does not own the copyright for those files. Only the copyright owner has the legal right to distribute such material. So each time someone downloads a copy from someone who is sharing they are violating the copyright for that file.

For more on copyright see:

http://www.ncsu.edu/copyright/ & http://oit.ncsu.edu/p2p
"What risks am I taking by using peer-to-peer file sharing software?"

Among others:

1. Students, faculty and staff may be criminally prosecuted and subject to civil litigation if it is used to infringe copyright.

2. Students may be suspended or expelled from school, and faculty and staff may be dismissed from their jobs.

3. Using file sharing applications exposes your computer to viruses that may cause irretrievable loss of data.

4. Your personal and/or confidential information may be inadvertently shared across the Internet."
Legal Alternatives

There are an ever increasing number of legal ways to view and purchase music and movies online. Although these eliminate the concern of copyright infringement they may not be appropriate when using University supplied computers.

.streaming Audio
  - Pandora - 40 hours free per month, $.99 for unlimited access per month.
  - Radio Station Websites

.streaming Video
  - Hulu
  - Crackle

.Network Websites: NBC, CBS, ABC, Comedy Central

.Online purchase
  - Apple iTunes
  - Amazon
  - Walmart
Use of Computing Facilities
for Commercial, Advertising, & Broadcast Purposes
Use of Computing Facilities

Paid Advertising

• No paid advertising will be allowed on official University Websites. However, an NC State Website may contain a simple acknowledgment of sponsorship by an outside entity in the following form: “Support for this Website [or university unit] has been provided by______.”

• “An "official University Website" is any World Wide Web address sponsored or endorsed or created on authority of a University department or administrative unit. Websites on University servers are either "University Websites" or personal Websites allowed by the University.

• "Paid advertising" means advertising or promotional information provided in exchange for money or any valuable benefits.
Use of Computing Facilities

“Personal Web pages maintained by University computer account holders may not contain paid advertising. This guideline is consistent with the University policy against use of University resources for private gain or commercial purposes.”

“Personal Web pages” are only websites hosted on University servers. If a user pays to host a website on non-University servers, or has a site on a free service such as Facebook, WordPress, or MySpace, they are not affected by these policies.

Ads placed by University employees on external Internet sites may not refer readers to a University telephone number or university e-mail address.
Use of Computing Facilities

Broadcast Emails

Bulk email usage, other than that required for legitimate university business or intra-unit communications, is not endorsed by the university.

- “University computer account holders may not "broadcast" E-mail messages without prior approval from a University official with the rank of Chancellor, Provost, Vice Chancellor for Information Technology, or their designees. "Broadcast," means transmission of an unsolicited message to a significant number of computer accounts on a University server or servers; the intent is to prevent mass mailings from tying up employee time and computer resources.

- Will not be considered “broadcast” e-mail under this section:
  - The use of emails by university units to reach their constituency or
  - The use of authorized university e-mail lists for their intended purpose.
Use of Computing Facilities

University Trademarks

“Registered marks of the University as designated by the NCSU Trademark Licensing Office may be used in the Websites of University computer account holders on the conditions that:

1. They are not used for or related to private profit or commercial purposes, and
2. They do not mislead or confuse viewers as to whether the Web page is University-sponsored.”
Violation of Policy
Violation of Policy

Employees
• “Any violation of these policies by employees may be "misconduct" under EPA policies (faculty and EPA non-faculty), or "unacceptable personal conduct" under SPA policies.

Students
• For students, violations are misconduct under the applicable student disciplinary code.

Approved Guests
• Violations will result in appropriate action depending on their affiliation.
Violation of Policy

Sanctions

• Violators may be referred to the appropriate disciplinary university procedure, as well as criminal or civil prosecution.
• Sanctions may include revocation of access privileges in addition to other sanctions.
• Apart from referrals to disciplinary procedures, an authorized University system administrator (or designees) may suspend a user's access privileges or suspend services to a computer, for as long as necessary to protect the University's computing resources, to prevent an ongoing threat of harm to persons or property, or to prevent a threat of interference with normal University functions.
• Systems administrator designees will have sufficient IT background and training to understand the technical issues being addressed in the proceedings.
Violation of Policy

As soon as practicable following the suspension of access privileges, the system administrator must take the following actions:

• The user must be sent written or electronic notice of the suspension of access and the reasons for it, and notice of the time, date, and
• Location at which the suspension may be discussed with the system administrator.
Violation of Policy

The user must be given an opportunity to meet with the system administrator at his or her earliest convenience to discuss the suspension and present any reasons the user has why the suspension should be lifted. The system administrator must reconsider his or her suspension decision in light of the information received at this meeting.

Following the meeting, the user must be sent a copy of the system administrator's decision upon reconsideration, and must be notified that the user may appeal to the system administrator's immediate supervisor if the user is dissatisfied with the outcome of the meeting.
Application of Public Records Law
Application of Public Records Law

Duty to Preserve Records

- All information created or received for University work purposes and contained in University computing equipment files, servers or electronic mail (e-mail) depositories are public records and are available to the public unless an exception to the Public Records law applies.

- As with hard-copy documents, e-mail users are responsible for the retention of e-mail messages that have lasting or archival value in accordance with the N.C. Public Records Law and NC State University's published guidelines regarding records retention and disposition.

- The university has created an email archive for the university central email systems using the Postini archive service.
Application of Public Records Law

Duty to Preserve Records Continued

This archive is provided as an authoritative source of email public records for the email user or for the university to answer legitimate requests for the information contained in the emails.

Duty to Provide Access to Information Content

Employees and approved guests with a network account or University computing device must provide decryption, passwords, and any other appropriate assistance when an identified University official (e.g., supervisor or person in employee's chain of command) needs access to any of the university's records/data the employee may have stored on university machines, systems, or storage devices, or on non-university machines, systems, or storage devices.
Application of Public Records Law

Additional Duty Regarding Records Requests & Potential Litigation

• Any University employee or authorized guest (e.g., volunteers and students serving in a University office) who receive notice of a public record request or possible lawsuit or other legal claim must promptly
  • Notify the Office of General Counsel of the request or possible claim, and
  • Locate and preserve all relevant records.
Additional Rules
Additional Rules

Additional rules on computer use may be adopted by various divisions/departments to meet specific administrative or academic needs. Any adopted requirement must:

- Comply with applicable federal and state laws;
- Be consistent with the policies of NC State and the University of North Carolina;
- Be posted in writing or electronically in a manner and in an approved format that is available to all affected users; and
- Be filed with the Office of General Counsel, and the Vice Chancellor for Information Technology (CIO).
Some additional recommendations from the Security team:

- Servers or SANs should not be used for storing personal files.
- Users should not create personal accounts not related to the business purpose of the server on a University server.
Thank You for Completing the Training