Norwich University
Information Technology Acceptable Use
&
Electronic Communications Policy

Contents

Introduction

Norwich University's Information Technology Department provides extensive Information Technology and Electronic Communications resources to support the University's education, research, and service missions. By accepting and/or using any Information Technology and Electronic Communications Resources, here after referred to as IT/EC Resources, the user understands and agrees to this Policy.

1. Purpose

1.1 The purposes of this Policy are to:

- Establish an Information Technology Acceptable Use & Electronic Communications Policy,
- Ensure that the University's IT/EC Resources support the University's education, research, and service missions,
- Ensure that IT/EC Resources are used in compliance with applicable State and Federal laws and University policies,
- Provide additional Administrative Interpretation that serves as guidance to the meaning of this Policy.

2. Scope

2.1 This Policy applies to:

- All IT/EC Resources owned, managed, or utilized by the University, which includes, but is not limited, to:
    - Computers,
    - Networks,
    - Networking equipment,
    - Wireless equipment,
    - Databases,
    - Servers,
    - Storage Systems,
    - Internet, Intranet, and Extranet resources,
    - Electronic mail (email),
    - Electronic bulletin/notice boards,
    - Electronic discussion/news groups,
    - Instant Messaging and 'chat' facilities,
    - Electronic calendars.

- All Information Technology Resources not specifically owned, managed, or utilized by the University, but connected to University IT/EC Resources (ie. Personal computers).
- The users of Norwich University IT/EC Resources, which includes, but is not limited to, all:
    - Students,
    - Employees,
        - Full-time and part-time Faculty,
        - Full-time and part-time Staff,
          ROTC personnel,

- Temporary Employees,
- Volunteers,
- Guests
  - Special Events,
  - Summer Camps.

2.2 Campus Units that operate their own IT/EC Resources may add, with the approval of the Vice President of Technology & Strategic Partnerships, individual guidelines, which supplement, but do not relax, the policies stated here.

2.3 Any omission of an IT/EC Resource or Record in this Policy does not implicitly or explicitly grant anyone access to that Resource or Record and/or authorize abandonment of common sense and civility in the use of that Resource or Record.

2.4 Any comments or questions about this policy shall be directed to the University's Information Security Officer at extension 2456.

3. Definitions

3.1 Definitions for the terms used in this Policy are defined in Appendix A. Users of the University's IT/EC Resources are expected to understand the definitions as they are applied to this Policy.

4. Responsibilities

4.1 It is the responsibility of the Information Technology Department to ensure that the persons to whom this Policy applies are appropriately aware of this Policy.

4.2 Use of the University's IT/EC Resources is a privilege, not a right, and as such it is the individual's responsibility to abide by this Policy.

4.3 Non-compliance with this Policy may result in the suspension or termination of the IT/EC Resources if, in the Vice President of Technology & Strategic Partnerships' judgment determines, a violation by a user has occurred.

5. Policies

5.1 Academic Purpose Use

The University's IT/EC Resources are provided to support the University's education, research, and service missions and as such all IT/EC Resources shall be used in a manner that supports the University's mission and goals. It is however, understood that users may need to utilize the University's IT/EC Resources for personal use. Personal use should be limited and not interfere with valid University usage. For further clarification of excessive personal use see the Violations section, Excessive Personal Use subsection below.

5.2 Accounts

Access to IT/EC Resources may require an account and shall be granted to active University employees (faculty and staff) and students.

Inactive or idle accounts, accounts not used for 45 days, will be locked or disabled. Locked accounts will require contacting the User Support Help Desk at extension 2456 for re-activation. In the event that an IT/EC Resources account is locked the account will still continue to receive records.

Temporary accounts shall be created for individuals or groups external to Norwich University, which require access to IT/EC Resources. Temporary accounts will be created under the following conditions:

- A full-time Norwich employee places the request for the temporary account(s) at least one week prior to the start of the event or conference and is responsible for any and all activity related to the training including any activity with or on the training accounts,
- The request for an account is for a conference or event sponsored by Norwich University,
- Any group will present the required $1M insurance rider as required by the University,
- Any Information Technology or Electronic Communications resource must be tested prior to the conference during weekdays.
- Temporary accounts will be removed at the end of the event and will not be available outside of the Norwich network.

Users are responsible for their accounts and are not to be shared with other users.

5.3 Authorized Access

You shall only access IT/EC Resources that are publicly available, information that is your own, or to which you have been given authorized access. Any attempt to gain unauthorized access to any IT/EC Resources or record is strictly forbidden.

Users must recognize that they are accountable for activities or material on their computer and must take appropriate actions to protect themselves. Such actions include, but not limited to,

- Logging off their computer when not in use,
- Locking their desktop when their computer is not in use,
- Shutting down their computer when it is not in use,
- Utilizing a password protected screen saver.

If an IT/EC Resource is left unattended and logged into, permission is not implicitly or explicitly granted to anyone accessing that device-either the account or the resources associated with that account.

5.4 Administrative Data

Administrative data includes, but is not limited to, academic transcripts, Norwich University financial information, student and employee billing information, alumni giving, human resources records including payroll, admissions records and financial aid data.

Administrative Data exists in several forms including electronic, hard copy and the memories of people. The guarding of this information means protecting a valuable Norwich asset and protecting the confidentiality of the person who entrusted Norwich with that personal information. Addresses, phone numbers, employment history, personal financial and medical histories as well as salaries, GPAs and disciplinary records are all stored on University IT/EC Resources and transferred between authorized users by electronic or other means. Securing this information at all stages is the responsibility of everyone.

Users should access only those data and transactions required to conduct their officially assigned duties. "Browsing" of records is prohibited. Access to a set of records is not authorized access to all records. Access to administrative systems is granted to a particular individual based on the need to use specific data, as defined by job duties, and subject to appropriate approval. Employees (including work study) who attempt unauthorized access to administrative computer access IDs are subject to disciplinary measures. Any individual who has been given authorized access to any information is not to make or permit unauthorized use of any information.

Before releasing information, ask if you are authorized to release the information to the requesting party. Users must safeguard the dissemination of information by phone, fax or printed materials to those approved to receive the data. Improper access to or unauthorized disclosure of confidential information may be a violation of federal law. Any individual who has been given authorized access to any information is to require proper identification before discussing information pertinent to the individual's record.

Printed output containing confidential or sensitive information must be treated with the same care as confidential data files. Floppy disks and cartridges must be stored in a locked file cabinet or desk; disks with sensitive information must be locked in a cabinet with a non-standard key lock. Shred or burn paper or microfiche copies to ensure the security of the information. Properly discard computer disks (hard disks and floppy) containing administrative information; Mac disks must be re-initialized but other PC disks require a more sophisticated utility to remove access to the data. All hard copy collections of information that are restricted in access must be clearly labeled as such.

In addition to protecting electronic and hard copy distribution of data, data must be protected from inadvertent "view" access. Monitor screens must be oriented to prevent unauthorized people from reading sensitive information. Any individual who has been given authorized access to any information is to assure that the virtual display devices will be protected from casual use or observation by unauthorized persons.

Supervisors shall periodically review the security access of their staff by ensuring that staff have properly secured administrative information-by turning off computers, clearing desktops and returning materials to secure locations. Storage of non-electronic forms of administrative information must safeguard against the information's unauthorized viewing as well as loss due to accidents or acts of nature.

Supervisors are responsible for establishing guidelines for the management and protection of data in their area in conjunction with the Information Technology department. The University's Information Security Officer can assist with developing guidelines, policies, and procedures.

Any departmental guidelines may supplement this policy, but may not relax or supersede it.

5.4.1 Student Records

Norwich University student education records are protected under the Norwich University's Academic Regulations and the Family Educational Rights and Privacy Act (FERPA). Under FERPA, students shall have the right to inspect and review education records, the right to request education records be corrected if it is believed that the education records are inaccurate, and the right to have some control over how the education records are disclosed.

5.5 Passwords and Password Maintenance

All IT/EC Resources accounts require passwords. It is the user's responsibility to choose passwords that are not easily accessible by others, which includes, but is not limited to

- Stored electronically,
- Written down either electronically or by traditional means,
- Easily recognizable passwords,
- Sharing passwords with anyone.

Unless otherwise stated, users shall perform password maintenance regularly and in compliance with the guidelines stated in this Policy.

Passwords shall be:

- Changed at least every six months,
- At least eight characters,
- Created with both an uppercase and lowercase character,
- Created with a number and special character such as ! @#$%,

Strong passwords are often created with a phrase, affirmation, or even a song title. As an example "This is one way to remember a password" could be created into a password like Tilw2rap!

Passwords shall not be:

- Not found in the dictionary,
- A common usage word such as the following,
  - names of family members, pets, co-workers etc,
  - the names Norwich, Northfield or any derivative or any other common word associated with Norwich University,
  - personal information such as birthdays, addresses, or telephone numbers,
  - common word or number patterns such as qwerty, 1234567,
  - any of the above spelled backwards,

- any of the above with a number in front or back of the password.

Interception or decryption of any passwords is strictly prohibited. Use of any IT/EC Resource or Personal Resource to intercept or decrypt any passwords is strictly prohibited.

5.6 Resources

Users of IT/EC Resources shall be sensitive to the needs of others and understand that everyone is sharing limited resources (ie. Bandwidth, storage space). Users must make reasonable efforts to use IT/EC Resources in a way that does not negatively affect others.

The Information Technology Department reserves the right to restrict, disallow, or limit access to IT/EC Resources to ensure legitimate activity and resource allocation that supports the University's education, research, and service missions. In the event that resources are restricted, disallowed, or limited users will be notified in a timely manner and will be restored as soon as the event is determined to no longer exist.

IT/EC Resources may be periodically audited either electronically or in person by Information Technology staff. Every effort will be made to limit auditing at a time that may be disruptive during normal working hours. In the event that an IT Resource can not be located, the last known user and/or supervisor may be contacted during normal working hours to located the IT Resource.

5.7 Personal Resources

Personal Resources may be allowed to connect to IT/EC Resources. In the event that a device or resource is connected to the University network, authentication and/or registration (either electronically or written) shall be required. In the event that a peripheral device (ie. printer) is connected to an Information Technology Resource, the peripheral device shall be clearly marked with the owner's information (ie. Name and department).

Personal Resources may be audited--either electronically and/or in person by Information Technology staff and/or Authorized Individuals--for security purposes or as required by law. Individuals are expected to comply with and not interfere with Information Technology staff and/or Authorized Individuals during the process.

Faculty and staff who would like to use their Personal Resources need to make a written request to the Computer Services Help Desk at helpdesk@norwich.edu. In the event of a manual registration, verification of antivirus software, current operating system patch level, and network interface card's MAC address must be supplied to an Information Technology staff member. Proof of software licenses may be required, in the event of a University wide software audit.

Reasonable efforts shall be made to provide general network/Internet connectivity; however, general hardware and software support is not guaranteed on Personal Resources.

Network support for Faculty and Staff Personal Resources shall be provided only after Student support requests and University owned Faculty and Staff support requests have been fulfilled.

The use of personal servers and/or networking equipment is strictly prohibited on the Norwich University network. Personal servers and networking equipment includes, but not limited to,

- Email server(s),
- Web server(s),
- Database server(s),
- Print server(s),
- Storage server(s),
- DHCP server(s),
- Firewall Server(s),
- Switches,
- Router(s),
- Wireless Access Point(s),
- Port mappers, network sniffers, and/or other network discovery tools, software, or devices.

5.8 Public Facilities Resources

Users shall not prevent others from using shared Public Facility Resources by locking or placing "reserved" or "hold" signs on the Resource. Use of the Public Facilities Resource is prioritized:

- Highest: academic, course-related work,
- Medium: personal productivity (including non-course-related text processing and E-mail),
- Lowest: recreational computing (including web browsing and game playing).

Those using the Public Facilities Resources for the lowest priority computing, must relinquish these computers to those requiring them for higher priority work. No food or drink is permitted in Public Computing Resource areas (ie. computer labs).

In order to permit other computer users to concentrate on their work, conversation should be conducted elsewhere.

5.9 Software Resources

The Information Technology Department purchases and maintains Software Resources. To ensure compliance with licensing and copyrights laws, all original software media (ie. disks, cdroms) will be inventoried and stored in the Information Technology department. Many Software Resources adhere to strict licensing agreements and may require auditing, either electronically or in person, by Information Technology staff.

Users shall not install any application or software, including by not limited to,

- Freeware,
- Shareware,
- Screensavers,

• Games

onto University owned Information Technology Resources without the prior permission of the Vice President of Technology & Strategic Partnerships or University's Information Security Officer.

Any software determined to be in violation of this Policy or federal copyright laws shall be removed immediately. Future violations may be subject to limitation, suspension, or termination of Information Technology Resources.

The Information Technology Department does not supply or support software on personally owned Information Technology Resources.

5.10 Copyright and Copyright Infringement

Copyright material of third parties, (ie. software, music, movies, cartoons, images, text) shall not be distributed in Information Technology and Electronic Communications without specific authorization from the originator or creator. Specific authorization shall be provided to the Vice President of Technology & Strategic Partnerships or University's Information Security Officer upon request.

Distributing, copying, downloading, sharing or saving copyright material may give rise to personal and/or University liability under applicable State and Federal laws. In the event of an investigation the University will fully comply with law enforcement officials, which may include, but not limited to, providing personal information and/or IT/EC Records.

5.11 Expectation of Privacy

University IT/EC Resources are the property of Norwich University and users have no expectation of privacy when utilizing IT/EC Resources, even if the Resources are used for personal purposes. IT/EC Resources and Records may be monitored and/or logged by authorized Information Technology staff and users shall not assume that their IT/EC Resources and/or Records are private. IT/EC Records may include, but not limited to, email, instant messages, chat, intranet and/or Internet traffic.

The Information Technology Department will make every reasonable effort to protect Electronic Communications Records from unauthorized access, viewing, or inspection.

IT/EC Records and Administrative Data will not be shared with external, non-Norwich affiliated individuals, groups, and/or vendors.

5.12 Monitoring / Logging

Periodically, Information Technology Staff or Authorized Persons may need to monitor and/or log IT/EC Resources or Records. Normal monitoring and/or logging may be required for operational, maintenance, compliance, auditing, or security purposes. Any monitoring and/or logging required for investigative purposes will only be done with the prior approval of the Vice President for Technology and Strategic Partnerships.

5.13 Law Enforcement Requests

Any Law Enforcement requests for IT/EC Resources and/or Records, searches, and/or interrogation shall follow the University's standard recommendation-a valid subpoena is required.

5.14 Illegal, Harassing, or Offensive Material

This Policy works in conjunction with, but does not relax, the University's Non-Discrimination and Sexual Assault and Sexual Misconduct Policies. IT/EC Resources shall not be used contrary to any State or Federal laws, which includes, but not limited to, harassment, offensive, obscene, disruptive, defamatory, racially vilifying, pornographic, or unlawfully discriminatory material.

5.15 Viruses

The Information Technology department provides and maintains antivirus software for all IT/EC Resources. The IT department can also supply antivirus software to all students.

All data, files, or software shall be checked with an anti-virus software program before being launched, opened, or accessed. Do not download any files, email, or attachments that you are not expecting or that appears to be suspicious. If you receive any files, email, or attachments that you suspect have a virus, report the occurrence immediately to the User Support Help Desk at extension 2456 or helpdesk@norwich.edu for further assistance.

IT/EC Resources found to be infected with a virus, worm, Trojan horse, or other malicious code must be disconnected from the Norwich University network immediately to prevent further contamination of other IT/EC Resources. Student IT Resources that are infected or suspect to be infected can bring their computer to the NUCERT shop located in Juckett Hall room 014 for assistance.

In order to protect IT/EC Resources and/or the University network, the Information Technology Department may disconnect any or all networking / Internet capabilities by client, computer, port, building, dormitory, or residence hall. In the event that networking and/or Internet connectivity is disconnected, the University community shall be notified in a timely manner of the downtime and approximately when the connectivity shall be restored.

5.16 Attribution / False Attribution

Electronic Communications has the risk of false attribution-meaning it is possible that IT/EC Records may be created or modified to reflect a false sender, recipient or message. Users may be unaware that they are receiving fraudulent information. If you suspect that an IT/EC Record is suspicious or fraudulent please contact the User Support Help Desk at extension 2456 or helpdesk@norwich.edu.

5.17 Mass Distribution

Using IT/EC Resources to mass distribute IT/EC Records (ie. junk mail, for-profit messages, or chain letters) is strictly prohibited.

5.18 Complaints

If you receive an internal or external Electronic Communications Record, which is offensive or inappropriate please contact the User Support Help Desk at extension 2456 or helpdesk@norwich.edu.

5.19 Records Management

Retention of Electronic Communications Records (ie. email) may utilizing large amounts of disk storage space and can affect system space and performance. It is your responsibility to perform routine records management, which may include periodically deleting email that no longer has usefulness. If you need help or training on email management you can contact the User Support Help Desk at extension 2456 or helpdesk@norwich.edu.

5.20 Backups

Electronic Communications records (ie. email) are backed up on a regular basis solely for the purpose of system integrity, reliability, or disaster recovery. Backups are not provided for future incidental retrieval.

5.21 Violations

Violations or breaches of this Policy will be categorized using the following guidelines. The categories below may not represent all conceivable situations and situations not covered below will be dealt with on a per case basis.

- Illegal
  This category involves activities or material considered to be in violation of State or Federal laws including, but not limited to, child pornography or copyrighted material. Law enforcement officials will be notified and utilized to resolve illegal violations of this Policy.

- Critical
  This category involves activities or material that is generally offensive in nature including, but not limited to, racial or religious vilification, unlawfully discriminatory, defamatory, or sexual harassment. Appropriate University officials will be utilized to resolve critical violations.

- Extreme
  This category involves activities or material that reasonable adults would consider to offend against standards of morality, decency, or generally accepted by adults. Appropriate University officials and/or supervisors will be utilized to resolve extreme violations of this Policy.

- Excessive Personal Use

  - During working hours
    This category involves activities that occur during normal working hours, adversely affects the performance of the University employee(s), and is more than insignificant.

  - Outside working hours

This category involves activities that occur outside of normal working hours and accounts for more than 2 hours on a particular day.

Users found to be in violation of excessive personal use will be reported to their immediate supervisor and/or the appropriate University official. If repeated violations occur, IT/EC Resources may be suspended, limited, terminated, or revoked, whichever action is found to be appropriate by the Vice President of Technology & Strategic Partnerships.

5.22 Policy Updates

This Policy shall be updated in accordance with the University's Procedures for Enacting Additions, Changes and Deletions.

Appendix A, Definitions

Account(s): Any Information Technology or Electronic Communications related username or login ID. Accounts are owned by Norwich University and shall be used for institution related activities.

Electronic Communications: Any electronic form of communication that is broadcast, circulated, propagated, sent, transmitted, copied, forwarded, replied to, created, stored, displayed, viewed, read, or printed by any Electronic Communications, Resource, Systems, or Services.

Electronic Communications Record(s): Any form of an electronic transmission, file or message that is broadcast, circulated, propagated, sent, transmitted, copied, forwarded, replied to, created, stored, displayed, viewed, read, or printed by any Electronic Communications Resource, Systems or Services.

Electronic Communications Resources: Any combination of Information Technology equipment including, but not limited to, computers, servers, networks, storage systems, data processing systems, and related software, programs, and computer records that supports Electronic Communications Services.

Electronic Communications Systems or Services: Any system or service that depends on Electronic Communications Resources to broadcast, circulate, propagate, send, transmit, copy, forward, reply to, create, store, display, view, read, or print any Electronic Communications Record(s).

Information Technology: Any aspect of creating, exchanging, operating, processing, managing, storing, and/or using information in its various forms by any Information Technology Resource.

Information Technology Resource: Any application, device, physical or virtual asset, software, or property used to support Information Technology.

Personal Resources: Any combination of Information Technology equipment including, but not limited to, computers, laptops, handheld devices, and/or printers (non-networked).

Personal Use: Any usage of IT/EC Resources beyond normal University sanctioned activity that does not support the University's education, research, and service missions.

Appendix B, References

Norwich University Policies and Guidelines:

Academic Regulations - FERPA
http://www.norwich.edu/policy/academic/appendix3.html

Non-Discrimination Policy -
http://www.norwich.edu/policy/discrimination/index.html

Sexual Assault and Sexual Misconduct Policy -
http://www.norwich.edu/policy/sexualassault/index.html

Procedures for Enacting Additions, Changes and Deletions -
http://www.norwich.edu/policy/administrative/changes.html

Vermont Statutes:

Title 13: Crimes and Criminal Procedure, Chapter 87: COMPUTER CRIMES
http://www.leg.state.vt.us/statutes/sections.cfm?Title=13&Chapter=087

Federal Statutes and Regulations:

Americans with Disabilities Act of 1990 -
http://www.usdoj.gov/crt/ada/

Communications Decency Act of 1996 -
http://www.cdt.org/speech/cda/951221cda.html

Copyright Act of 1976 -
http://www.copyright.gov/titlel7/

Digital Millennium Copyright Act of 1998 -
http://www.copyright.gov/legislation/dmca.pdf

Electronic Communications Privacy Act of 1986 -
http://cio.doe.gov/Documents/ECPA.HTM

Family Educational Rights and Privacy Act of 1974 -
http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Privacy Act of 1974 -
http://www.usdoj.gov/foia/privstat.htm

Telecommunications Act of 1996 -
http://www.fcc.gov/telecom.html

Federal Communications Commission Rules and Regulations -

http://www.fcc.gov/

Electronic Freedom of Information Act Amendments of 1996
http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm

Health Insurance Portability and Accountability Act of 1996 -
http://aspe.hhs.gov/admnsimp/p1104191.htm

Sarbanes-Oxley Act of 2002 - http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3763enr.txt.pdf

Gramm-Leach-Bliley Act of 1999 -
http://www.senate.gov/banking/conf/confrpt.htm