UNG
UNIVERSITY of NORTH GEORGIA™

University of North Georgia

2013

Appropriate Usage Policy

Division of Information Technology

Version 1.0

Unrestricted

Revision & Sign-off Sheet

Change Record

Date	Author	Version	Change Reference

Reviewers

Name	Version Approved	Position	Date
Alfred Barker	1.0 - Approved	CISO	01/28/2013
Brandon Haag	1.0 - Approved	CIO	01/28/2013
Jenna Colvin	1.0 - Approved	Legal Representative	02/05/2013
IT Leadership	1.0 Approved	Governance Review	02/06/2013
Jill Holman	1.0 Approved	Internal Audit	02/19/2013

Distribution

Name	Location
Backup Copy	Dunlap Mathis Building, Rm. 132 (Fire-Rated Safe)
Original Copy	DM, Rm. 129 (CISO's Office)
Electronic Copy	https://my.ung.edu/departments/InfoSec/ (Secure Portal)

Document Properties

Item	Details
Document Title	*Appropriate Usage Policy*
Document Type	Policy – Internal/Operational
Author	Alfred Barker
Document Manager	Alfred Barker
Creation Date	12/04/2012
Last Updated	01/28/2013
Document Classification	Unrestricted

1.0 Executive Summary

Respect for intellectual labor and creativity is vital to academic discourse and enterprise at the University of North Georgia (the "University"). This principle applies to works of all authors and publishers in all media, which includes respect for the right to acknowledgment, the right to privacy, and the right to determine the form, manner, and terms of publication and distribution. Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and copyright violations, may be grounds for sanctions against members of the academic community.

The University's expectation is all information technology resources are utilized in a responsible manner, respecting the public trust through which these resources have been provided, the rights and privacy of others, the integrity of facilities and controls, state and federal laws, and USG policies and standards. Moreover, the University strives to provide an environment that encourages the free exchange of ideas and sharing of information. Access to this environment and the University's information systems is a privilege and is to be treated with the highest standard of ethics.

2.0 Governance / Compliance / Authority

The University's *Information Security Program Policy* establishes the governance, compliance, and authority required to define appropriate usage. The following documents and policies support this definition:

- *Board of Regents Policy Manual* - Section 11 "Information Technology (IT)"
- Board of Regents *Business Procedures Manual* - Section 12 "Protection and Security of Records"
- Board of Regents *Information Technology Handbook* - Section 5.8.1 *USG Appropriate Use Policy* and Section 5.8.2 *USG AUP Interpretation and Administration Guideline*
- *PeachNet Acceptable Usage Policy*
- *Georgia Computer System Protection Act* - O.C.G.A. § 16-9-90 & HB1630
- Georgia's *Obscenity and Related Offenses* – O.C.G.A § 16-12-80
- Federal *Family Educational Rights and Privacy Act* (FERPA-20 U.S.C. § 1232g; 34 CFR Part 99)

3.0 Continuance

This policy may be reasonably modified at any time by the Chief Information Officer/Chief Information Security Officer (CIO/CISO) of the Division of Information Technology (hereinafter "IT") or the President and/or the cabinet of the University. This document replaces the *Information Systems Acceptable Use Policy* v2.1 (NGCSU-Revised 2010) and the v2.0 *Computer and Network Usage Policy* v1.2 (GSC-Revised 2009).

4.0 Scope

This policy outlines the standards for the appropriate usage of the University's information technology resources, which include, but are not limited to, equipment, software, wired or wireless networks, data, and telephones whether owned, leased, or otherwise provided by the University (hereinafter "IT Resources"). In addition, this policy is binding and applies to all University employees, students, or affiliates located on but not limited to the facilities at Cumming, Dahlonega, Gainesville, and Oconee (hereinafter "Users").

5.0 Requirements/Responsibilities

To establish the requirements of appropriate usage, this instrument constitutes a University-wide policy intended to define the appropriate use of all University IT Resources, effective protection of users, equitable access, and proper management of those resources which should be taken in the broadest possible sense. These guidelines are intended to supplement, not replace, all existing laws, regulations, agreements, and contracts that currently apply to these services.

Access to University IT Resources imposes certain responsibilities and obligations and is granted subject to University policies and local, state, and federal laws. Appropriate use should always be legal, ethical, reflect academic honesty, reflect community standards, and show restraint in the consumption of shared resources demonstrating respect for intellectual property; ownership of data; system security mechanisms; and individuals' rights to privacy and to freedom from intimidation, harassment, and unwarranted annoyance. Appropriate use of IT Resources includes instruction; independent study; authorized research; independent research; communications; and official work of the offices, units, recognized student and campus organizations, and agencies of the University.

5.1 Expectations

Users are expected to abide by the following standards of appropriate and ethical use:

- Use only those IT Resources for which you have authorization;
- Protect the access and integrity of IT Resources;
- Abide by applicable local, state, federal laws, University policies;
- Respect the copyrights and intellectual property rights of others, including the legal use of copyrighted material;
- Use IT Resources only for their intended purpose;
- Respect the privacy and personal rights of others; and
- Do no harm.

5.2 Definitions

5.2.1 Authorized Use

Authorized use of the University IT Resources is consistent with the education, and service mission of the University, and consistent with this policy.

5.2.2 Authorized Users

Authorized Users are: (1) current faculty, staff, and students of the University; (2) anyone connecting to a public information service; (3) others whose access furthers the mission of the University and whose usage does not interfere with other Users' access to resources.

5.3 Individual Privileges

It is the following individual privileges, all of which currently exist at the University, that empower each of us to be productive members of the campus community. It must be understood that privileges are conditioned upon acceptance of the accompanying responsibilities.

5.3.1 Privacy

To the greatest extent possible in a public setting, the University will strive to preserve individual privacy. Users must recognize that the University's IT Resources are public and subject to the *Georgia Open Records Act*. Users, thus, utilize such systems at their own risk. Electronic and

other technological methods must not be unreasonably used to infringe upon privacy. Any and all information systems activities may be logged, monitored, and/or reviewed. The University will not resell, distribute, or provide access to any collected information except where permitted by policy, contract, or state or federal law.

5.3.2 Freedom of Expression

The constitutional right to freedom of speech applies to all members of the University no matter the medium used.

5.3.3 Ownership of Intellectual Works

In accordance with O.C.G.A § 50-18-70, information stored or transmitted using University IT Resources is subject to open and transparent disclosure and is governed by the University System of Georgia unless otherwise specified in contractual or legal requirements. For protection, users creating intellectual works using the University IT Resources, should consult *Determination of Rights and Equities in Intellectual Property* (Board of Regents Policy Manual, Section 6.3.3) and any subsequent revisions, and other possibly related University policies. The University maintains the rights to access, obtain, review, or disclose this information when it is deemed necessary or required by law. Users are responsible for recognizing (attributing) and honoring the intellectual property rights of others.

5.3.4 Freedom from Harassment, Display of Objectionable or Undesired Material

All members of the University have the right not to be harassed by computer and wired or wireless network usage of others. *(Reference: 5.4.3 Harassment)*

5.4 Individual Responsibilities

Just as certain privileges are given to each member of the University community, each User is held accountable for his or her actions as a condition of continued membership in the community. The interplay of privileges and responsibilities within each situation engenders the trust and intellectual freedom that form the heart of our community. This trust and freedom is grounded on each user developing the skills necessary to be an active and contributing member of the community. These skills include an awareness and knowledge about the technology used to process, store, and transmit data and information.

5.4.1. Common Courtesy and Respect for Rights of Others

Users are responsible to all other members of the campus community in many ways, including respecting and valuing the rights of privacy for all, recognizing and respecting the diversity of the population and opinion in the community, behaving ethically, and complying with all legal restrictions regarding the use of information that is the property of others. Users shall employ information systems in a cordial and respectful manner and may not create an intimidating, hostile, or offensive environment through use of these resources. Additionally, Users shall not use information systems to transmit communications that are fraudulent, defamatory, harassing, obscene, threatening, that unlawfully discriminate or that are prohibited by law.

5.4.2. Privacy Requirements

Users of the University IT Resources will make every reasonable effort to ensure the privacy of the information entrusted to the University by its students, employees, vendors, guests and external organizations. The University shall take reasonable steps to secure and monitor systems storing sensitive or confidential information to ensure the privacy of University constituents. Unprotected or insufficiently protected systems should be reported by Users to their supervisors or to the Division of Information Technology for assessment and remediation. Files of personal information, including programs, no matter on what medium they are stored or transmitted, may

be subject to the *Georgia Open Records Act* if stored on the University IT Resources. That fact notwithstanding, Users should not look at, copy, alter, or destroy another User's personal files without express permission (unless authorized or required to do so by law or regulation). Simply being able to access a file or other information does not imply permission to do so. Similarly, Users should not connect to any local host on the wired or wireless network without authorization or advance permission. People and organizations link computers to the wired or wireless network for numerous different reasons, and many consider unwelcome connects to be attempts to invade their privacy or compromise their security.

5.4.3 Harassment

No User or other member of the University community may, under any circumstances, use the University's IT Resources to libel, slander, or harass any other person. The following shall constitute Computer Harassment: (1) Using the IT Resources to annoy, harass, terrify, intimidate, threaten, or offend another person by conveying or publicly displaying obscene language, pictures, or other materials; (2) Using the IT Resources to convey threats of bodily harm to the recipient or the recipient's immediate family; (3) Intentionally using the IT Resources to contact another person repeatedly with the intent to annoy, or harass, whether or not any actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease; (4) Intentionally using the IT Resources to contact another person repeatedly regarding a matter for which one does not have a legal right to communicate, once the recipient has provided reasonable notice that he or she desires such communication to cease (such as debt collection); (5) Intentionally using the IT Resources to disrupt or damage the academic, research, administrative, or related pursuits of another; (6) Intentionally using the IT Resources to invade the privacy, academic or otherwise, of another or the threatened invasion of the privacy of another.

5.4.4 Responsible Use of Resources

IT Resources, including paper, are for **Academic and Administrative Use Only**. Users are responsible for knowing what information resources (including wired or wireless networks) are available, remembering that the members of the University community share them, and refrain from all acts that waste or prevent others from using these resources or from using them in ways that have been proscribed by the University. Users shall be responsible for ascertaining that the use of IT Resources complies with all University and University System of Georgia/Board of Regent policies. The University prohibits the intentional accessing, downloading, printing, or storing of information with sexually explicit or other illicit content unless it can be demonstrated that such content is reasonably intended to contribute to academic inquiry. Users shall be responsible for complying with all state and federal laws when using information systems including all relevant copyright laws. Additionally, Users shall not use information systems in such a way that violates the University's contractual obligations, including limitations defined in software or other licensing agreements.

5.4.5 Information Integrity

It is the responsibility of the User to be aware of the potential for and possible effects of manipulating information, especially in electronic form, to understand the changeable nature of electronically stored information, and to verify the integrity and completeness of information that is compiled or used. Users are not to depend on data or communications to be correct when it appears contrary to expectations; users should question and/or verify all data exchanges with the person who they believe originated the communication.

5.4.6 Use of Desktop Systems

Users are responsible for the security and integrity of University information stored on personal desktop systems. This responsibility includes controlling physical and network access to the machine; avoiding storage of passwords or other information that can be used to gain access to other University IT Resources. The individual exercise of backups on local systems or on removable media for university-related business where the data may be classified as sensitive or confidential is prohibited unless otherwise addressed in policy. The use of approved/provided shares is encouraged; exceptions are personal data.

5.4.6.1 Faculty and Staff use of Network Shared Folders

Faculty and staff are encouraged to use the approved and provided network shared folder space referenced from the University workstations. By doing so, the faculty and staff ensure the availability of their files from any University computer on campus and will find these files are also made available off campus via remote access. Access to these files requires a user name and password. An additional benefit is it allows the IT staff to provide protection of the documents through the use of tape backups and the operating system's backup/recovery technology. This technology gives the IT staff or Help Desk personnel a tool to recover documents that may have been lost, corrupted, or deleted. Saving work on the workstation's local drive(s) does not provide this form of disaster recovery or file accessibility and is highly discouraged.

5.4.6.2 Student Use of the Networked Shared Folders

Students are encouraged to store their information in the approved network share or on removable media, which serves as the students' backup protection. By doing so, the students ensure the availability of their files from any University computer and will find these files are also made available off campus via remote access. Students are encouraged not to store data anywhere else other than the network share (or removable media). Storing on the network share allows the IT staff to provide a level of disaster recovery protection to the documents through the use of tape backups and a tool to recover documents that may have been lost, corrupted, or deleted. To access these files the student must have a username and password.

5.4.7 Access to Facilities and Information

5.4.7.1 Sharing of Access

The University maintains the right to access, obtain, review, or disclose information when it is deemed necessary or required by law. Otherwise, computer accounts, passwords, and other types of authorization are assigned to individual Users and must not be shared with others.

5.4.7.2 Permitting Unauthorized Access

Users may not run or otherwise configure software or hardware to intentionally allow access to unauthorized users. *(Reference Section 5.2.1 Authorized Use.)*

5.4.7.3 Use of Privileged Access

Special access to information or other special computing privileges are to be used in performance of official duties only. Information that is obtained through special privileges is to be treated as private.

5.4.7.4 Termination of Access

When Users cease being a member of the University community (cease enrollment or terminate employment), or if Users are assigned a new position and/or responsibilities within the University, access authorization must be reviewed and terminated if appropriate. Users must

refrain from using facilities, accounts, access codes, privileges, or information not explicitly authorized.

5.4.8 Attempts to Circumvent Security

Users are prohibited from attempting to circumvent or subvert any system's security measures. Exceptions include security tools utilized by systems and security administration personnel in the course of business.

5.4.8.1 Decoding Access Control Information

Users are prohibited from deploying any computer program or device to intercept or decode passwords or similar access control information.

5.4.8.2 Denial of Service

Deliberate attempts to degrade the performance of the IT Resources or to deprive authorized personnel of resources or access to any University computer system and wired or wireless network is prohibited.

5.4.8.3 Harmful Activities

Creating or propagating viruses; disrupting services; running unauthorized wired or wireless equipment; damaging files; intentional destruction of or damage to equipment, software, or data belonging to the University or other Users is defined as harmful activities and are prohibited. Users shall not perform wired or wireless network scans, probes, or deploy monitoring services or software without appropriate permission. Users shall not misrepresent themselves as someone else, or intentionally damage or destroy equipment, software, or data.

5.4.9 Academic Dishonesty

Users should always use IT Resources in accordance with the high ethical standards of the University community. Academic dishonesty (plagiarism, cheating) is a violation of those standards.

5.4.10 Use of Copyrighted Information and Materials

Users are prohibited from deploying, inspecting, copying, and storing copyrighted computer programs and other material, in violation of federal and state copyright laws.

5.4.11 Use of Licensed Software

No software may be installed, copied, or used on University IT Resources except as permitted by the owner of the software in conjunction with prior review and approval from the Division of Information Technology. Software subject to licensing must be properly licensed and all license provisions (installation, use, copying, number of simultaneous users, term of license, etc.) must be strictly adhered to.

5.4.12 Political Campaigning; Commercial Advertising

Board of Regents Policy Manual (Section 9.10.6.1) states "The use of System materials, supplies, equipment, machinery, or vehicles in political campaigns is forbidden." The use of University IT Resources shall conform to these policies.

5.4.13 Personal Business

University IT Resources may not be used in a manner that violates the Non-Solicitation Policy or in connection with compensated outside work or for the benefit of organizations not related to the University, except in connection with traditional faculty pursuits such as teaching, research and service. This and any other incidental use (such as electronic communications or storing data on

single-user machines) must not interfere with other Users' access to IT Resources (computer cycles, network bandwidth, disk space, printers, etc.) and must not be excessive. State law restricts the use of State facilities for personal gain or benefit.

5.4.14 Game Playing

The University shall provide designated areas to be used for recreational game playing, computer chatting, and role-playing, not including any form of gambling. These activities are not permitted on any computer or within any lab that has not been approved. The privilege of using University IT Resources for game playing, chatting, or role-playing depends upon the civility of the Users. Should there be impoliteness, rowdiness or other unpleasantness, this privilege may end immediately.

5.4.15 Reporting Violations

Users shall report all violations of this policy as well as any potential criminal activities or information security issues to IT or anonymously online.

5.5. University Privileges

Our society depends on institutions like the University to educate our citizens and advance the development of knowledge. However, in order to survive, the University must attract and responsibly manage financial and human resources. Therefore, the University has been granted by the State, and the various other institutions with which it deals, certain privileges regarding the information necessary to accomplish its goals and to the equipment and physical assets used in its mission.

5.1. Allocation of Resources

The University may allocate resources in differential ways in order to achieve its overall mission.

5.2. Control of Access to Information

The University may control access to its information and the devices on which it is stored, manipulated, and transmitted, in accordance with federal and state laws, and policies governing the Board of Regents and the University. The University retains the right to revoke access to IT Resources.

5.3. Imposition of Sanctions

The University may impose sanctions and punishments on Users and other members of the University community who violate this and other policies of the University regarding IT Resources usage.

5.4. System Administration Access

System Administrators (i.e., the personnel responsible for the technical operations of computer systems) may access others files for the maintenance of networks and computer and storage systems, such as to create backup copies of media, or any official function. However, in all cases, a User's privileges and rights of privacy are to be preserved to the greatest extent possible.

5.5. Monitoring of Usage, Inspection of Files

The University may routinely monitor and log usage data, such as wired or wireless network session connection times and end-points, CPU and disk utilization for each user, security audit trails, network loading, etc... in the course of performing an official function. In all cases, a User's privileges and rights of privacy are to be preserved to the greatest extent possible. The University does not routinely monitor individual use of information systems, but most Internet-based activities are logged. The University does maintain the rights through its authorized agents

to actively access, obtain, collect, maintain, and review information concerning any use or access to IT Resources.

5.6. Suspension of Individual Privileges

The University of North Georgia may suspend computer and wired or wireless network privileges of a User for reasons relating to his/her physical or emotional safety and wellbeing, or for reasons relating to the safety and wellbeing of other members of the University community, or University property. Access will be promptly restored when safety and well being can be reasonably assured, unless access is to remain suspended as a result of formal disciplinary action imposed by the Office of the Vice President for Student Affairs (for students) or the employee's unit lead in consultation with the Office of Human Resources (for employees).

5.6. University Responsibilities

5.6.1. Security Procedures

The University has the responsibility to reasonably develop, implement, maintain, and enforce appropriate security procedures to ensure the confidentiality and integrity of individual and institutional information, however stored, and to impose appropriate penalties when privacy is purposefully abridged.

5.6.2. Anti-Harassment Procedures

The University has the responsibility to reasonably develop, implement, maintain, and enforce appropriate procedures to discourage harassment by use of its IT Resources and to impose appropriate penalties when such harassment takes place.

5.6.3. Upholding of Copyrights and License Provisions

The University has the right to uphold all copyrights, laws governing access and use of information, and rules of organizations supplying information resources to members of the University community.

5.6.4. Public Information Services

Units and Users may not configure wired or wireless computing systems to provide information retrieval services to the public at large. (Current examples include "ftp servers", "web servers", “peer-to-peer file sharing” and “wireless access points”.) If this type of access is necessary, the Division of Information Technology will provide it. However, in so doing, particular attention must be paid to the following sections of this policy: 5.*2.1 Authorized Use* (authorized use must be consistent with University mission), 5.*3.3 Ownership of Intellectual Works*, *5.4.4 Responsible Use of Resources*, *5.4.10 Use of Copyrighted Information and Materials*, and *5.4.11 Use of Licensed Software*. The use of public services must not cause computer or network loading that impairs other services.

6.0 Sanctions/Enforcement

It is recommended that employees, students and affiliates be informed of what constitutes appropriate use of the University’s IT Resources. To support this recommendation, the *Appropriate Use Policy* strives to define the standards of appropriate conduct. Failure to comply with this and all other Information Technology policies may result in revocation of privileges and/or actions as specified in the University’s Human Resources *Progressive Disciplinary Policy*. IT is not responsible for issuance of sanctions greater than the violation notifications and removal of computer and wired or wireless access.

6.1 Procedures and Sanctions

Specific guidelines for interpretation and administration of the *USG Appropriate Use Policy* are given in the *USG AUP Interpretation and Administration Guideline*. In addition, the following guidelines contain more specific examples of offenses, and procedures for dealing with incidents: USG *Appropriate Use Policy*; Student Disciplinary Policy; Human Resources' *Progressive Discipline Policy*.

6.2 Investigative Contact

A User, who is contacted by a representative from an external organization (District Attorney's Office, FBI, GBI, AT&T Security Services, etc.) who is conducting an investigation of an alleged violation involving the University IT Resources, must inform the Chief Information Officer/Chief Information Security Officer immediately.

6.3 Enforcement

Failure to comply with this Policy may result in revocation of privileges and/or actions as specified in the University's Human Resources *Progressive Disciplinary Policy*, Faculty Handbook, and/or Student Handbook. All reports of student violations will be directed to the appropriate Dean of Students per campus. First violation reports for employees will be directed to the employee's supervisor. Subsequent faculty violations will be directed to the Provost; subsequent staff or administrative violations will be directed to Human Resources. Any information related to illegal or suspicious activity will be directed to Public Safety for contact with the appropriate law enforcement agency.

6.3.1 First and Minor Incident

If a User appears to have violated this policy, and (1) the violation is deemed minor by IT, and (2) the person has not been implicated in prior incidents, then the incident may be dealt with at the IT or unit level. The alleged offender will be furnished a copy of the *Appropriate Usage Policy* (this document), and will sign a statement agreeing to conform to the policy.

6.3.2 Subsequent and/or Major Violations

Reports of subsequent or major violations will be forwarded to Student Affairs (for students) or the unit head (for employees) for the determination of sanctions to be imposed. Units should consult Human Resources regarding appropriate action.

6.4 Range of Disciplinary Sanctions

Users in violation of this policy are subject to the full range of sanctions, including the loss of IT Resources access privileges, disciplinary action, dismissal from the University, and legal action. Some violations may constitute criminal offenses, as outlined in the *Georgia Computer Systems Protection Act* and other local, state, and federal laws; the University will carry out its responsibility to report such violations to the appropriate authorities.

6.5 Appeals

Appeals should be directed through the already-existing procedures established for employees and students.

7.0 Responsibilities/Review

All compliance, documentation, enforcement and maintenance of this Policy are the responsibility of IT and are stored within IT's fire-rated safe, online within the University's secure portal, and in working form within the office of the Chief Information Security Officer. This policy is to be used to establish the definition of appropriate use of the University's IT Resources. It is recommended that the content and execution of this policy be audited at a

minimum by the Chief Information Security Officer annually, at which time this policy may be updated as appropriate.