Status **Active** PolicyStat ID **13583062**

Last Approved	10/2023
Effective	10/2023
Last Revised	10/2023
Next Review	10/2026
Owner	Jason Matt: Sr. VP for Business Operations & Chief Operating O
Area	University Wide
References	Policy

Information Technology Acceptable Use Policy

I. POLICY PURPOSE

This policy serves to establish the expectations for the use of Information Technology (IT) resources at the University of North Georgia (the "University"), to prohibit unacceptable uses, and to educate users about their individual responsibilities and the University's privileges.

II. DEFINITIONS

A. **Authorized Users**

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.

B. **Information Technology (IT) Resources**
Any facilities, equipment and services owned, operated or provided by contract to the University or Affiliated Organizations for the use of members of the University community. By way of example, this includes e-mail and telecommunications systems, information technology systems, traditional and electronic bulletin boards, computers, mail, websites, broadcasts, fax machines, and copiers/printers. Information Technology Resources also 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).

C. **Public Record**
All documents, papers, letters, maps, books, tapes, photographs, computer-based or generated information, data, data fields, or similar material prepared and maintained or received by an agency or by a private person or entity in the performance of a service or function for or on behalf of an agency. To include even when such documents have been transferred to a private

person or entity by an agency for storage or future governmental use.

III. POLICY STATEMENT

A. This policy is binding and applies to all Authorized Users.

B. Acceptable Use
Acceptable Use of University IT Resources includes any purpose related to the direct and indirect support of the University's educational, research, service, student and campus life activities, and administrative and business purposes. Authorized Users are provided access to IT Resources to support their studies, instruction, research, duties as employees, official University business, and other University-sanctioned activities according to their roles and responsibilities.

C. Unacceptable Use
Authorized Users must not engage in Unacceptable Use of University IT Resources, which includes but is not limited to the following:

1. Sharing or transferring authentication details to others, or using another user's authentication credentials such as network IDs and passwords, or other access codes or circumventing user authentication that could allow unauthorized users to gain access to University IT Resources;
2. Violation of federal, state, or local laws; institutional policies, rules or guidelines; or licensing agreements or contracts;
3. Harassment of, threats to or defamation of others; creation of a hostile environment; stalking; and/or discrimination;
4. Intentionally damaging, disrupting, or exposing IT resources or data to unauthorized access or harm;
5. Storage, display, transmission, or intentional or solicited receipt of material that is or may reasonably be regarded as obscene, pornographic, except as such access relates to, University-related academic or research pursuits or as needed to investigate violations of University policy or laws;
6. Outside employment, commercial activities, or other forms of private financial gain;
7. Campaigning for public office or soliciting political contributions;
8. Political lobbying, except for specific employees designated to lobby on behalf of the University;
9. Use for private or personal purposes that interfere with work or job performance or that interfere with the activities of other employees, students, or other authorized users;
10. Authorized users must not use University IT Resources to speak on behalf of the University or use the University trademarks or logos without authorization. Affiliation with the University does not, by itself, imply authorization to speak on behalf of the University.

D. Individual Responsibilities
Access to this environment and the IT Resources is a privilege and is to be treated with the

highest standard of ethics. Authorized Users are expected to use IT Resources only for their intended purpose and to abide by guidance as defined by Acceptable and Unacceptable Use as well as the following standards of appropriate and ethical use:

1. Accountability – Each Authorized User is held accountable for his or her actions. Use only those IT Resources for which you have authorization and protect the access and integrity of IT Resources.
2. Privacy Requirements – Authorized Users of IT Resources will make every reasonable effort to ensure the privacy of the information entrusted to the University.
3. Public Records of the University, including those stored on IT Resources or personal devices, are subject to the Georgia Open Records Act. There should be NO expectation of privacy for material stored on the University's IT Resources.
4. Authorization – Users should not connect to any local host on the wired or wireless network without authorization or advance permission.
5. Harassment – No User may, under any circumstances, use the University's IT Resources to unlawfully harass any other person.
6. Responsible Use of Resources – IT Resources, including paper, are for University academic and administrative use only. Authorized users shall be responsible for ensuring that the use of IT Resources complies with all University and University System of Georgia/Board of Regent policies.
7. Authorized Users shall be responsible for complying with all state and federal laws, including all relevant copyright laws and intellectual property rights of others.
8. Authorized Users shall not use IT Resources in such a way that violates the University's contractual obligations, including limitations defined in software or other licensing agreements.
9. Computing Devices – Authorized Users are responsible for the security and integrity of University information stored on any device (University-issued devices or personal).
10. Attempts to Circumvent Security – Authorized Users are prohibited from attempting to circumvent or subvert any system's security measures.
    a. Subverting Security Measures –This includes, but is not limited to, using unapproved software for remote access or attempting to bypass network or host based firewalls. Exceptions include security tools utilized by systems and security administration personnel in the course of business.
    b. Harmful Activities
        i. Creating or propagating viruses; disrupting services; running unauthorized wired or wireless equipment; damaging files; interfering with, or otherwise impacting, wired, wireless or other institutionally owned infrastructure, 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.
        ii. Authorized Users shall not perform wired or wireless network

scans, probes, or deploy monitoring services, or connect to or install unapproved hardware or software without appropriate permission.

iii. Authorized Users shall not misrepresent themselves as someone else, or intentionally damage or destroy equipment, software, or data.

11. Non-University Business – University IT Resources are to be used for University business only, and Authorized Users are expected to adhere to the standards of Acceptable Use as defined above.
12. No one shall misrepresent his or her identity or relationship to the University when obtaining or using University computer or network privileges.
13. Reporting Violations – Authorized Users shall report all violations of this policy as required by the University Employee Handbook.

E. University Privileges

1. Allocation of Resources – The University may allocate resources in differential ways to achieve its overall mission.
2. Monitoring of Usage, Inspection of Files – Users should be aware that their use of university IT Resources is not private. While the University does not routinely monitor individual use of its IT Resources, the normal operation and maintenance of the university's IT Resources require the backup and caching of data and communications, the logging of activity, monitoring of general usage patterns and other activities necessary or convenient for the provision of service. Further, communications made by means of University IT Resources are generally subject to the Georgia Open Records Act and users should assume NO expectation of privacy. The University maintains the right through its authorized agents to actively access, obtain, collect, maintain, and review information concerning any use or access to IT Resources.
3. Suspension of Individual Privileges – The University may suspend computer and wired or wireless network privileges of an Authorized User for reasons relating to his/her physical or emotional safety and well-being, or for reasons relating to the safety and wellbeing of other members of the University community, or University property.

IV. SUPPORT INFORMATION

A. Governance / Compliance / Authority – The University's Information Security Program Policy establishes the governance, compliance, and authority required to define acceptable use. Nothing in this document should be taken to contradict policies, standards and guidelines made mandatory and binding by the University System of Georgia, the Board of Regents, the Georgia Technology Authority or other higher entity.

B. The following documents and policies support this definition:

1. *Board of Regents Policy Manual* - Section 11 "Information Technology (IT)"
2. Board of Regents *Business Procedures Manual* - Section 12 "Protection and Security

of Records"

3. 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*
4. *PeachNet Acceptable Usage Policy*
5. *Georgia Computer System Protection Act* - O.C.G.A. § 16-9-90 & HB1630
6. Georgia's *Obscenity and Related Offenses* – O.C.G.A § 16-12-80
7. Federal *Family Educational Rights and Privacy Act* (FERPA-20 U.S.C. § 1232g; 34 CFR Part 99)

C. Continuance – This policy may be reasonably modified at any time by the President of the University, their designee, or the responsible party. 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).

V. PROCEDURES

Any related operating procedures must comply with and should reference this policy.

Approval Signatures

Step Description	Approver	Date
Policy Office - Final Approval/ Posting	Wesley Burnett: Policy & Procedure Coordinator	10/2023
Office of the President	Jen Herazy: Senior Vice President of Strategy and Chief of Sta	10/2023
General Counsel	Elene Garrison: General Counsel	10/2023
	Mac McConnell: Sr. VP for Business & Finance	10/2023
Chief Information Officer	Steve McLeod: Associate Vice President and Chief Information Off	10/2023
Chief Information Security Officer	Rob Cherveny: Chief Information Security Officer	10/2023
Policy Office/Technical Review	Wesley Burnett: Policy & Procedure Coordinator	10/2023

Mac McConnell: Sr. VP for Business & Finance	05/2023