Information Resources Acceptable Use Regulation 508

Regulation 508 Approved: December 1, 2022

UNIVERSITY OF NORTH CAROLINA SCHOOL OF THE ARTS
INFORMATION RESOURCES ACCEPTABLE USE REGULATION 508

Source of Authority:	N.C.G.S. 116-34(a); *UNC Code* § 502(A)
Revision Authority:	Chancellor
History:	First Issued: February 17, 2011 Revised: March 24, 2022 Revised: December 1, 2022
Related Policies and Regulations:	Business Continuity Plan Regulation 104; Code of Conduct & Discipline Regulation 802;

Emergency Management Regulation 701;
Improper Activities Reporting Regulation 114;
IT Account Management Regulation 503;
Takedown Notice Regulation 507;
Virtual Private Network (VPN) Regulation 510

Conflicts of Interest Policy 603
Prohibited Discrimination, Harassment, and Related Misconduct Regulation 121
Email Regulation 502
Information Technology Security Regulation 512

University of North Carolina System Policy, Information Technology Chapter, Information Technology Governance 1400.1
University of North Carolina System Policy, Information Technology Chapter, Information Security 1400.2
University of North Carolina System Policy, Information Technology Chapter, User Identity and Access Control 1400.3

Responsible Offices:	Information Technology Department
Effective Date:	December 1, 2022

I. Purpose

This regulation sets forth the acceptable use of information resources at the University of North Carolina School of the Arts

(UNCSA). Information resources and that data contained in those resources are provided for university-related purposes and access to and use of information resources entails specific expectations and responsibilities for users as outlined in this policy.

II. Scope

This regulation applies to all university information resources, regardless of form or location, and the hardware and software resources used to electronically store, process, or transmit that information. This includes data processed or stored and applications used by the university in hosted environments in which the university does not operate the technology infrastructure. All UNCSA employees, students, and affiliates must adhere to this regulation.

III. Compliance

All UNCSA employees, students, and affiliates must adhere to this policy and related regulations, procedures, rules, standards, technical specifications, and any other guidance produced by the information security program. Failure to do so may result in disciplinary action, up to and including dismissal, suspension or expulsion, or termination of privileges.

IV. Definitions

A. **Affiliate** - An affiliate is an individual who requires access to information resources to work in conjunction with the university, but is not a UNCSA employee or student. Affiliates must have a sponsor who is an employee.

B. **Information Resources** - As used in UNC System Policy 1400.1, "information resources are information owned or processed by the university, or related to the business of the university, regardless of form or location, and the hardware and software resources used to electronically store, process or transmit that information." Information resources expressly include data, software, and physical assets.

V. Regulation

A. University information resources are owned by the university and are primarily provided for university-related purposes. University information resources must be used in a manner consistent with the university's academic, teaching, learning, artistic, cultural, economic, campus life, public service, and administrative missions.

B. The use of university information resources is a privilege and not a right. Members of the university community are expected to be good stewards of the university's information

resources and data, and use them in a safe, responsible, ethical, and legal manner. The continuing ability to use these resources is contingent upon their appropriate and responsible use.

C. All users of university information resources must abide by the following standards of behavior regarding information resources use:

1. Comply with all federal, State of North Carolina, and other applicable laws, regulations, contracts, including university or third party copyright, patents, trademarks, software license agreements.

2. Comply with all university policies, regulations, and rules regarding electronic communications, protection of institutional data, and the operation and use of information resources.

3. Use only those information resources and data that they have been authorized to use, and use them only to the extent authorized and in a manner that is consistent with the missions of the university.

4. Only store university data on information resources, devices, and cloud services provided by the university and in the manner specified by the university.

5. Automatic forwarding of university mail (e.g., from unsca.edu) to an outside third party mail system (e.g., gmail.com, yahoo.com, etc.) is prohibited for any correspondence that contains data classified as level 1 (confidential data), level 2 (sensitive data), or level 3 (controlled data).

6. Do not use information resources, including official university email lists or listservs, to send messages or material that are fraudulent, harassing, threatening as described in Prohibited Discrimination, Harassment, and Related Misconduct Regulation 121, or otherwise in violation of law or university policy.

7. Do not use information resources, including official university email lists or listservs, to engage in political activity, campaign for or against a ballot initiative or candidate running for office, or conduct a political campaign.

8. Refrain from creating the appearance that the university is endorsing, affiliated with, or otherwise supporting any

organization, product, service, candidate, or position.

9. Do not send unsolicited mass communications unrelated to university business, activities, or events unless permitted by Email Regulation 502.

10. Do not use information resources for personal commercial purposes or personal financial or other gain, except as permitted by Conflicts of Interest Regulation 603.

11. Refrain from disproportionate uses of information resources that have the likelihood of consuming an unreasonable amount of resources, disrupting the intended use of these resources, or impinging on the access of others.

12. Do not interfere with the intended use or proper functioning of information resources, or gain or seek to gain unauthorized access to any information resources or data contained on university information resources.

13. Do not circumvent or bypass security measures, requirements, or any standard protocols in place to ensure the confidentiality, integrity, and availability of university

information resources, data, information technology systems, and networks.

14. Promptly report potential information security incidents to the IT Networking and Information Security Department.

D. Incidental personal use of information resources is permissible to the extent that it does not:

1. Unreasonably interfere with the use of information resources by other users, or with the university's operation of information resources;

2. Interfere with the user's employment or other obligations to the university;

3. Violate any law or regulation; or

4. Violate this or other applicable university policy, regulation, procedure, or rule.

E. Users have no expectation of privacy in connection with the use of university information resources. The normal operation and maintenance of the university's information resources require backup and caching of data and communications, the

logging of activity, monitoring of general usage patterns, and other such activities. While university personnel does not routinely monitor the content of communications or transmissions using information resources, the university may, with or without further notice to users, take any action it deems necessary to preserve, protect and promote the interests of the university, its information systems, or university data. The university may access and monitor its information resources for any purpose consistent with the university's duties or mission without notice.

F. Any personally-owned devices used for university business are subject to this policy and must comply with all university policies, rules, and regulations about that type of device and to the type of data involved. Such resources must also comply with any additional security requirements specific to the university functions for which they are used.

A personally-owned device for purposes of this regulation is defined as any device not owned by the university that is capable of storing data and connect to a network, including but not limited to computers, tablets, phones, etc. If a personal device is used to access university systems and/or data, you must adhere to the following:

1. University data must be stored in a cloud system or other file storage owned by the university.

2. University data may not be stored on local, personally-owned resources such as computer hard drives, USB drives, external hard drives, phones, or other non-university storage or computing devices.

3. No employee, student, or affiliate using his or her personal device should expect any privacy except that which is governed by law.

4. UNCSA will not be responsible for loss or damage of personal devices, applications or data resulting from the use of company applications or network.

5. The UNCSA IT department reserves the right to remotely remove institutional data from personal devices such as email, cloud data, or other information for security purposes.

6. The university reserves the right to limit access or block personal devices from the university network at any time for security purposes.

G. The university makes no warranties of any kind, whether expressed or implied, concerning the information resources that it provides. The university is not responsible for damages resulting from the use of information resources, including but

not limited to loss of data resulting from delays, non-deliveries, missed deliveries, service interruptions caused by the negligence of a university employee, or by any user's error or omission. The university specifically denies any responsibility for the accuracy or quality of information obtained through information resources, except material that is presented as an official record of the university.

H. Roles and Responsibilities

1. All users of information resources are responsible for the appropriate use of information resources and data as described in this document.

2. The Chief Information Officer is responsible for administering this policy and providing guidance to senior leadership concerning the appropriate use of information resources.

3. The Director of Networking and Information Security shall be responsible for guiding the university's information security program and associated activities.

V. Revision History

A. February 17, 2011 – Adopted by Board of Trustees as part of UNCSA Policy Manual

B. March 24, 2022 - Revised to clarify the acceptable use of information resources.

C. December 1, 2022 - Revised to further define personally-owned devices subject to this regulation.