Acceptable Use of Computing and Electronic Resources Policy

Policy 906

1 Introduction

1.1. The purpose of this policy is to outline the acceptable uses and specific prohibitions that are inherent to the access and use of Information Technology and Information Resources owned or provided by Appalachian State University (hereinafter “the University”).

1.2. Individuals subject to this policy are responsible for exercising reasonable good judgment with respect to specific expectations regarding the use of Information Resources. Each user is expected to understand that Information Technology represents a shared service with finite resources. Users should exercise reasonable efforts to avoid impacting others’ efficient use of Information Technology and Resources.

2 Scope

2.1 Individuals Covered by this Policy

This policy applies to all users of Information Resources owned or provided by the University, including: 1) devices provided by the University, 2) services provided by the University, or 3) data that belongs to the University regardless of the location. This applies to any cloud services employed to conduct University business or provide University services.

3 Definitions

3.1 Administrative Control

protecting an information system through policy, procedure, training, directives from an authority, or similar efforts that instruct and require individuals to take corrective actions.

3.2 Authorized Personnel

an employee with assigned responsibilities to support Information Resources, or approved by the Office of General Counsel, Director of Human Resources or the Chief Information Officer or designee(s) to perform a specific duty or duties in regards to Information Resources.

3.3 Information Resources

information owned or possessed 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.

3.4 Information Technology

hardware and software resources owned, leased, or used by the University and its partners to store, process or transmit University information. Information technology is a subset of the University’s Information Resources.

3.5 ITS

the University’s Office of Information Technology Services.

3.6 IT Infrastructure

the system of enterprise hardware, software, networks, facilities, and service components used to develop, test, operate, monitor, manage, and/or support information technology services.

3.7 University

Appalachian State University.

3.8 User

a person who uses Information Resources.

4 Policy and Procedure Statements

4.1 Acceptable Uses

4.1.1 Individuals subject to this policy are responsible for exercising good reasonable judgment regarding what is the acceptable use of Information Technology and Information Resources. Generally, acceptable uses include, but are not limited to, the following:

1. Lawful uses not otherwise prohibited by UNC System or University policies.
2. Use of Information Technology and Information Resources to conduct University business.
3. Personal use of University maintained Information Technology that does not violate prohibitions listed in 4.2.7.
    1. The University shall not be responsible for any personal material or information stored on University Information Technology. The University assumes no responsibility for backing up personal material or personal information stored on University Information Technology and shall have no obligation to produce any such personal material or information at any point during or after an individual's period of employment, enrollment, or other affiliation. The user accepts all responsibility of removing personal materials prior to their separation with the University. This provision does not apply to current students' academic work stored on University Information Technology.

4.2 Prohibitions

4.2.1 Individuals subject to this policy are responsible for understanding that specific activities are prohibited unless a written exception is agreed to and provided by the Chief Information Officer or his delegate.

4.2.2 Users may not attempt to intentionally hide their identity for malicious purposes. All use of University Information Technology must be identified as to the individual or device using the system. Obfuscation or intentional misrepresentation of identity (e.g., shared credentials, spoofed communications, etc.) for any malicious purpose, including access to and use of Information Technology, is prohibited.

4.2.3 Users may not intentionally attempt to expand or offer IT infrastructure services to others, through the implementation of unapproved hardware, software or cloud services. The infrastructure may not be extended or otherwise modified without the oversight and approval of ITS. This includes, but is not limited to, servers that provide services to multiple users, network communications devices, multi-user storage devices, or network-based camera systems.

4.2.4 Users residing in residence halls may be subject to additional prohibitions as defined by University Housing.

4.2.5 Users, excluding authorized personnel, may not intentionally attempt to intercept, monitor, redirect, alter or otherwise adversely impact another user's use of University Information Resources. Users, excluding authorized personnel, may not read, copy, or delete another user's electronic data without the expressed prior approval of said user.

4.2.6 Users may not engage in cyberstalking, harassment or infringe upon the privacy of other users' lawful use of University's Information Resources.

4.2.7 Users may not intentionally engage in any activity that negatively impacts Information Resources.

4.2.8 Employees' personal use of Information Resources in accordance with 4.1.3 above may not 1) interfere with an employee's job performance, 2) interfere with activities that directly support the University mission, 3) violate UNC System and University policies including, but not limited to, policies prohibiting the use of University Information Technology and Information Resources to endorse, campaign for, secure support for or oppose any candidate, political party, partisan political group, referendum, or issue in an election; or 4) constitute use of Information Resources to seek commercial gain or private profit, except as allowed under applicable University policies including policies concerning intellectual property rights and external professional activities for pay. Supervisors have discretion to further restrict or forbid personal use as they reasonably deem necessary.

4.2.9 Users may not engage in any activity that intentionally circumvents administrative controls or in any way attempts to gain or provide unauthorized access to Information Resources.

4.2.10 Additional activities that are prohibited, specific to certain types of use such as Network Access, Storage, etc. may be described in other more specific standards located at https://its.appstate.edu/it-governance/it-policy-standards-guidelines

4.3 Additional Conditions of Use

4.3.1. By activating one's University user account, the user agrees to receive via email University security breach notifications required by the N.C. Identity Theft Protection Act, as well as other official University communication.

4.3.2. Departments may enforce additional administrative controls concerning use, as long as such controls are in accordance with this and other University policies and are within the scope of their assigned areas of oversight.

4.4 IT Security and Monitoring

4.4.1 The University does not routinely monitor or access individual communications. Review or monitoring of the use of Information Resources is reasonably limited by scope, relevance and applicable law and University policy and may occur in the following circumstances if deemed necessary by authorized personnel:

1. in accordance with generally accepted, network-administration practices and to resolve IT support requests;
2. to prevent or investigate any actual or potential information security incidents and system misuse;
3. to investigate reports of violation of University IT policy;
4. to support, as authorized by the Office of General Counsel, investigations of violation of local, state, or federal law; violations of University policies; or to comply with legal requests for information (such as subpoenas and public records requests); or
5. to retrieve information in emergency circumstances where there is an imminent threat to health, safety, or University property involved.

4.5 Enforcement

4.5.1 The University, in consultation with its legal counsel, may contact local or federal law enforcement authorities to investigate any matter in its sole discretion. Information Technology Services, in cooperation with other University authorities, is charged with enforcement of this policy, and establishing standards, procedures, and protocols in support of the policy.

4.5.2. To report a concern regarding non-compliance with this policy, please contact cio@appstate.edu

4.5.3. Penalties for violating this Policy may result in termination of or suspension of access, in whole or in part, to University Information Resources at the discretion of ITS where such action is reasonable to protect the University or University Information Resources. Failure to comply with this policy may put Information Resources at risk and may have disciplinary consequences for employees and students. Contractors, vendors, and others who fail to adhere to this policy may face termination of their business relationships with Appalachian State University.

4.5.4. Violations of this policy, insofar as they might also violate other policies, may also be enforceable under the following provisions:

1. For students, the Code of Student Conduct.
2. For employees, "misconduct" under the Faculty Handbook and other EHRA policies governing faculty and non-faculty EHRA employees, including any appeal rights stated therein; or "unacceptable personal conduct" under SHRA policies, including any appeal rights stated therein.

4.5.5. Faculty, staff, and students accused of violating this policy will be informed of the alleged violation when the notification does not place further investigation(s) or remediation at risk. Faculty, staff, and students can appeal a revocation or suspension of access to the Chief Information Officer or their designee; and can utilize appeal mechanisms included in any applicable policies and codes.

5 Additional References

5.1. All users should be aware of these additional statues and regulations as they may directly impact the lawful use of University Information Resources.

1. North Carolina General Statute 14-190-1, Obscene Literature and Exhibitions
2. North Carolina General Statute 144-456, Denial of Computer Services to an Authorized User
3. North Carolina General Statute 143B-920, Department Heads to Report Possible Violations of Criminal Statutes Involving Misuse of State Property to the State Bureau of Investigation
4. U.S. Code Title 18, Section 1030, Fraud and Related Activity in Connection with Computers
5. Education Rights and Privacy Act of 1974, 20 U.S.C. 1232g
6. Title VII of the Civil Rights Act of 1964, 42 U.S.C. 2000e, et seq.
7. Title IX of the Education Amendments of 1972, 20 U.S.C. 1681, et seq.
8. North Carolina Human Resources Act, N.C.G.S. Chapter 126
9. North Carolina Public Records Act, N.C.G.S. Chapter 132
10. UNC System Records Retention and Disposition Schedule
11. Email as a Public Record in North Carolina

12. Appalachian State University Faculty Handbook
13. Appalachian State University Code of Student Conduct
14. Appalachian State University Policy 110 Discrimination, Harassment, Retaliation, and Sex-Based Misconduct
15. Appalachian State University Policy 908 E-mail As Official Means of Communication
16. Appalachian State University Policy 105.6 Public Records Requests
17. Appalachian State University Policy 604.7 Political Activities and Public Office Holding
18. Appalachian State University Policy 604.3 External Professional Activities of Faculty and Other Professional Staff
19. Appalachian State University Policy 604.5 Staff (SHRA) Employee Request for Approval to Engage in Outside Work

6 Authority

The UNC Policy Manual, Chapter 100.1, The Code, Section 502

7 Contact Information

Office of the Chief Information Officer (828.262.6278)

8 Original Effective Date

June 21, 2017

9 Revision Dates

May 1, 2019 (This revision repealed the previous version of Policy 901 “Use of Computer and Data Communications” and replaced it with a new Policy 901 “Acceptable Use of Computing and Electronic Resources Policy” and a recommended University Privacy Policy)