

Code of Computing Practices

I. General Principles

- A. This Code governs the use of computers, networks, and other computing resources at the Arkansas Department of Environmental Quality. These resources are provided by the Department to enhance the accomplishment of its mission. The Department is committed to computing and network systems that effectively meet the needs of its users.
- B. Individuals who are granted computing accounts or who use computing resources at the Department accept the responsibilities that accompany such access. Use of computing resources in violation of the regulations set forth in this Code will be referred to the immediate supervisor for review.
- C. Computers and networks can provide access to resources within and beyond the Department's computer system, including the ability to communicate with other users worldwide. Such open access is a privilege, and requires that individual users act responsibly. Use of computing and network resources should always be legal and ethical, and show restraint in the consumption of shared resources. It should demonstrate respect for intellectual property, ownership of data, system security mechanisms, the right to personal privacy, and to the right of individuals to freedom from intimidation and harassment.
- D. All federal and state laws, general state and Department regulations and policies, and Governor's Policy Directives are applicable to the use of computing resources. These include, but are not limited to, 20 U.S.C. § 1232g; the Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510 et seq.; the Arkansas Freedom of Information Act, Ark. Code Ann. §§ 25-19-101 et seq.; and state and federal computer fraud statutes, 18 U.S.C. § 1030 and Ark. Code Ann. §§ 5-41-101 et seq. Illegal reproduction of software and other intellectual property protected by U.S. copyright laws and by licensing agreements may result in civil and criminal sanctions.
- E. The Department's Web site is maintained on the Department's computer system by the Computer Services Division. No member of the Department may produce a Web page, electronic bulletin board, or any other such computer site that purports to be an official publication of the Department without the express permission of the Department's Director.

II Administration of Computing Resources

A. In General

- 1. The Department, in accordance with state and federal law and other Department policies, may control access to its information and the devices on which it is stored, manipulated, and transmitted.

2. The Department has the responsibility to: (a) develop, implement, maintain, and enforce appropriate security procedures to ensure the integrity and confidentiality of individual and institutional information, however stored; (b) uphold all copyrights, patents, licensing agreements, and rules of organizations that supply information resources to the extent that these do not conflict with other applicable laws and polices.
3. Responsibility for administering the Department's computing and network resources rests with the Computer Services Division.

B. System Administrators

1. A system administrator is any person in the Computer Services Division designated to maintain, manage, and provide security for the Department's computing resources, including computers, networks, and servers.
2. System administrators shall perform their duties fairly, in cooperation with the Department staff. They shall adhere to this Code and all other pertinent Department rules and regulations, shall respect the privacy of users to the greatest extent possible, and when necessary shall refer issues or instances of inappropriate use of resources to appropriate Department staff for review and potential disciplinary action.

C. Data Collection

1. Given the nature of the technology, a wide range of information can be collected by Department staff using system software. For example, software may be configured to provide aggregate information on the number of users logged in, the number of users accessing certain software, etc.
2. No information shall be routinely collected that is not required by system administrators in the direct performance of their duties, e.g., routine backups for system recovery, investigating error reports, etc.

D. Privacy of Electronic Files

1. Users do not own accounts on Department computers but are granted the privilege of exclusive use of their accounts. Use of the Department's computing resources for storage or transmission of data does not alter any ownership interest of the user in that data. Users are entitled to privacy regarding their computer communications and stored data to the greatest extent possible within the restrictions and exceptions of the laws, regulations, and policies described in this Code.
2. System administrators will access electronic files, including e-mail files, only as necessary to perform their duties. These duties include installation, enhancement, and maintenance of computers, networks, data, and storage systems; actions necessary to maintain the integrity of

the computers, networks, or storage systems; adding, removing, or modifying user accounts; or actions necessary to protect the rights or property of the Department or other users. Authorized personnel may routinely monitor and log usage data, such as network session connection times and end-points, CPU and disk utilization for each user, security audit trails, and network loading. E-mail messages which are rejected due to some error, e.g., defective addressing, may be reviewed to determine the nature of the error, the significance and immediacy of the rejected message, and what corrective action(s) might be necessary. In all cases, the privacy of users shall be protected to the greatest extent possible.

3. Because the Department is a public agency and all files must be available to satisfy potential FOIA requests, care must be taken when applying computer security procedures to protect files. Because of these accessibility requirements as they relate to the Department, the use of password protection methods on individual files is prohibited. This includes but is not limited to the procedures included in many PC-based word processing, spreadsheet, and database software that allow the user to apply a password to an individual file to restrict its accessibility. In the event that special protections on files are needed by a user or group of users, the Computer Services Division will assist the user or users in applying security methods that provide the necessary security while still allowing access by authorized personnel in order to satisfy the Department's accessibility requirements.

E. The Arkansas Freedom of Information Act

1. The electronic files, including e-mail files, of Department employees are potentially subject to public inspection and copying under the state Freedom of Information Act ("FOIA"), Ark. Code Ann. §§ 25-19-101 et seq.
2. The FOIA defines "public records" to include "data compilations in any form, required by law to be kept or otherwise kept, . . . which constitute a record of the performance or lack of performance of official functions which are or should be carried out by a public official or employee [or] a governmental agency. . . ." (See Ark. Code Ann. § 25-19-103(1).) All records maintained in public offices or by public employees within the scope of their employment are presumed to be public records; however, various exceptions apply. See Ark. Code Ann. § 25-19-105.

III. Use of Computing Resources

A. In General

This section does not cover every situation involving the proper or improper use of the Department's computing resources; however, it does set forth some of the responsibilities that a person accepts if he or she chooses to use those resources. The purpose of this section is to establish rules for the benefit of all

users and encourage responsible use of computing resources.

B. Use Without Authorization Prohibited

1. No one shall (a) connect with or otherwise use any Department computer, modem, network, or other computing resource without proper authorization; (b) assist in, encourage, or conceal any unauthorized use, or attempted unauthorized use, of any Department computer, modem, network, or other computing resource; or (c) misrepresent his or her identity or relationship to the Department to obtain access to computing resources.
2. No software can be installed on Department computers without prior review and approval by the chief of the Computer Services Division. This restriction is instituted to provide for adequate network and PC compatibility, reliability, and stability, to protect from computer viruses, and to ensure compliance with federal copyright laws. In general, only software purchased by and licensed to the Department, public domain software, or software which is copyrighted but distributed freely (e.g., computer magazine utility programs) will be installed.
3. Access to resources on the Internet is granted on an individual basis with a memo from the user's division chief or similarly positioned supervisor in the Director's Office.

C. Accounts

1. All computer resources shall be used in accordance with the general policies and procedures found in the Department's Employees Handbook and this Code.
2. Users shall not subvert restrictions associated with their accounts, such as privileges and levels of access.
3. No one shall give any password for any Department computer or network to any unauthorized person, nor obtain any other's person's password by any unauthorized means. Users are responsible for the use of their computer accounts and shall not allow others access to their accounts, through sharing passwords or otherwise except as necessary to perform assigned duties (but in no case to unauthorized persons). Users should take advantage of system-provided protection measures to prevent such access. Computer Services Division staff, in the performance of their duties, are authorized to request and use the accounts and passwords of other users.
4. When a user ceases being employed by the Department or is assigned a new position and/or different responsibilities within the Department, his or her account and access authorization shall be reviewed. A user shall not use facilities, accounts, access codes, privileges, or information for which he or she is not authorized.

D. Security and Related Matters

1. No one shall (a) knowingly endanger or compromise the security of any Department computer, network facility, or other computing resource or willfully interfere with others' authorized computer usage, (b) attempt to circumvent data protection schemes, uncover security loopholes, or decrypt secure data; (c) modify or reconfigure or attempt to modify or reconfigure any software or hardware of any Department computer or network facility in any way, unless specific authorization has been obtained; or (d) use Department computer resources and communication facilities to attempt unauthorized access to or use of any computer or network facility, no matter where located, or to interfere with others' legitimate use of any such computing resource.
2. No one shall attempt to access, copy, or destroy programs or files that belong to other users or to the Department except in the performance of assigned duties, nor shall anyone use Department computing resources for unauthorized monitoring of electronic communications.
3. No one shall create, run, install, or knowingly distribute a computer virus, Trojan Horse, or other destructive program, e-mail, or data via any Department computer or network facility, regardless of whether demonstrable harm results. No one shall alter, reconfigure, or remove the anti-virus software on any Department computer, except in performance of assigned duties.
4. The Department cannot guarantee the privacy of computer files, e-mail, or other information stored or transmitted by computer, including confidential information; moreover, the Department may access such information in accordance with Part II of this Code. Persons who have access to confidential or sensitive information shall disclose it only to the extent authorized by the Arkansas Freedom of Information Act, and other applicable laws, and only in connection with official Department business.
5. Users shall not knowingly or recklessly perform any act that will interfere with the normal operation of computers, terminals, peripherals, or networks and shall not intentionally waste or overload computing resources.

E. Electronic Property

No one shall copy, install, use, or distribute through the Department's computing resources any photographs, logos, images, graphics, graphic elements, audio, video, software, html markup, data files, or other information in violation of U.S. copyright, trademark, or patent laws or applicable licensing agreements. It is the user's responsibility to become familiar with the terms and requirements of any such laws or agreements.

F. User Communications

1. Users assume full responsibility for messages that they transmit through the Department's computers and network facilities.
2. No one shall use the Department's computing resources to transmit any material prohibited by law.
3. No one shall use the Department's computing and network resources to:
(a) annoy, harass, threaten, intimidate, terrify, or offend another person by conveying offensive language or images or threats of bodily harm; (b) repeatedly contact another person to annoy or harass, whether or not any actual message is communicated, and the recipient has expressed a desire for the contact to cease; (c) repeatedly contact another person regarding a matter for which one does not have a legal right to communicate (such as debt collection), once the recipient has provided reasonable notice that he or she desires such contact to cease; (d) disrupt or damage the work of another person; or (e) invade the privacy of another person or threaten such an invasion where such an invasion is not work-related and allowed by this Code.
4. When using the Department's computing resources, users shall comply with this Code as well as the regulations and policies of news groups, lists, and other public forums through which they disseminate messages.
5. Users shall not (a) initiate or propagate electronic chain letters; (b) engage in spamming or other indiscriminate mass mailings to news groups, mailing lists, or individuals; (c) forge communications to make them appear to originate from another person, e.g., spoofing; or (d) engage in resource-intensive activities unrelated to the Department's functions.

G. Listserv Lists

Approval for a listserv list based on the Department's computer system and which is available on the Internet must be obtained from the Director. If resources are available, such approval requires that the proposed list (a) not be a duplicate of an existing list, and (b) serve the mission of the Department.

IV. Enforcement and Sanctions

- A. System administrators are responsible for protecting the system and users from abuses such as described in this Code. Pursuant to this duty, system administrators may (1) formally or informally discuss the matter with the offending party, or (2) refer the matter to the appropriate disciplinary authority.
- B. Any violation of this Code may result in the revocation or suspension of access privileges as necessary to avert a degradation or interruption of service to the Department. As soon as possible, such action will be referred to the appropriate Deputy Director.

- C. Any violation of this Code is misconduct for purposes of personnel policies and may be punished accordingly.
- D. Any offense that violates local, state, or federal laws, or state or Department policies, may result in the immediate loss of all Department computing and network privileges and may be referred to the appropriate Department disciplinary authority and/or law enforcement agencies.

(Major portions of this Code were originally developed by the Computing Activities Council of the University of Arkansas at Fayetteville for use in the Code of Computing Practices at UAF. The contribution of the Council is gratefully acknowledged.)