Department of Transformation and Shared Services
State Cybersecurity Office

Policy Title: Information Technology Acceptable Use Policy
Policy Version: 1.0
Authority: A.C.A. § 25-4-110(c)
Effective Date: 8/23/2013

Information Technology Acceptable Use Policy

Purpose

Pursuant to Arkansas Code Annotated §25-4-110(c), concerning agency technology plans, the Information Technology Acceptable Use Policy (hereinafter "policy") is provided as follows: (a) to define the policy requirements; and (b) to define the acceptable and unacceptable uses of the Internet by state employees in the performance of their duties including but not limited to agency technology resources, social media and blogging for both business and personal reasons, and the use of electronic personal devices and resources at work or for work-related reasons.

The Arkansas Department of Information Systems (hereinafter "DIS") provides its staff with technology resources, equipment and a local area network with access to the Internet. The purpose of these technologies is as follows: a) to enhance DIS programs and services; b) to conduct DIS business and facilitate the efficient and productive use of the Internet as a means of accomplishing the mission and program goals of DIS; c) to support DIS projects; and d) to ensure that DIS staff are equipped with the necessary tools for communication, research, collaboration, and other tasks required to fulfill job obligations. Each DIS staff member is expected to use resources and accounts for these purposes. Access to the Internet is provided as a privilege and a tool for users who agree to act in an appropriate and responsible manner. All DIS staff must carefully review and adhere to the policy.

Policy

1. Appropriate Use of Technology

1.1. Technology as a required resource and privilege

Appropriate uses of technology include:

- Accessing the Internet for work related research and information gathering;
- Utility and applications software that accomplish tasks and fulfill job functions;
- Communication and collaboration between staff and/or other appropriate entities;
- Access to the Internet for up-to-date information published by DIS, other state agencies, schools, various other providers of information that may be necessary in order to complete job tasks;
- Activities or projects that support professional activities of employees.

1.2. Privacy of Information

Appropriate uses of technology concerning privacy of information include:

- DIS reserves the right to monitor and/or log all network activity with or without notice, including e-mail and all website communications, and therefore, users should have no reasonable expectation of privacy in the use of these resources.
- DIS will not monitor e-mail transmissions on a regular basis, though the construction, repair, operations and maintenance of electronic messaging systems may occasionally result in monitoring transmitted or stored messages.
- Messages may be monitored during the course of investigations of suspected illegal or prohibited activity, in order to respond to a Freedom of Information Act request, in order to respond to a discovery request or other legal process or proceeding, and when otherwise necessary to the operations of the agency.

1.3. User Restrictions

Brief and occasional personal use of the Internet is acceptable as long as it is not excessive or inappropriate, does not violate any of the prohibitions in Sections 1.4 and 3.3 below, does not result in additional expenses to DIS, and does not use significant network resources. Management reserves the right to determine whether any use is inappropriate, excessive, and/or violates the policy.

1.4. Unacceptable Uses

The following general uses are prohibited:

- Interference with the security or operation of the computer systems;
- Vandalizing equipment, software, or hardware;
- Attempting to alter or gain access to unauthorized files or systems;
- Integrating employee or personally-owned hardware, software or peripherals without DIS authorization. For additional information, refer to the Software and Hardware Policy ;
- Using technology in a way that interferes with work obligations;
- Violating the rights of others by publishing or displaying any information that is defamatory, obscene, inaccurate, profane, or threatening;
- Using, submitting, publishing, displaying, or transmitting on the network or on any computer system any information which:
    - Violates or infringes on the rights of any other person, including the right to privacy;
    - Contains defamatory, false, inaccurate, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, or otherwise biased, discriminatory, or illegal material;
    - Inhibits other users from using the system or the efficiency of the computer systems;
    - Encourages the use of controlled substances;
    - Uses the system for the purpose of criminal intent; or
    - Utilizes the system for any other illegal purpose.
- Using the facilities and capabilities of the system to:
    - Knowingly transmit material, information, or software in violation of any local, state or federal law;

- Conduct any non-governmental-related fund raising or public relations activities;
- Engage in any activity for personal financial gain, such as buying or selling of commodities or services with a profit motive;
- View, download or send pornographic or other obscene materials,
- Play or download games; or
- Adversely impact agency productivity.

1.5. Use of Flash Drive or Thumb Drive

No work product, data, documents or other information shall be saved or stored on a flash drive or thumb drive unless the drive is encrypted. Please refer to the **Encryption of Portable Data Policy** for more detailed information.

2. Electronic Mail (E-mail)

E-mail is considered network activity as well as state property and as such is subject to all policies regarding acceptable/unacceptable uses of information technology. The user should not consider e-mail to be either private or secure.

2.1. Purpose of e-mail

Electronic mail is provided to support open communication and the exchange of information between staff and other appropriate entities that have access to a network. This communication allows for the collaboration of ideas and the sharing of information. E-mail is a necessary component of teamwork at DIS.

It is the responsibility of the employee who is provided an e-mail account to use his/her account in accordance with his/her job duties.

2.2. Unacceptable use of e-mail

The following e-mailing conduct is prohibited:

- Any activity covered by inappropriate use statements included in this policy;
- Knowingly sending or forwarding chain letters, virus hoaxes, broadcast, spam, etc.;
- Sending, forwarding or opening executable files (.exe) or other attachments unrelated to specific work activities;
- Sending, soliciting, printing, copying or replying to text or images that disparage, offend or embarrass others based on sex, race, age, religion, national origin, veteran status, ancestry or disability;
- Use in messages of abusive, profane, or offensive language based on sex, race, age, religion, national origin, veteran status, ancestry or disability;
- Spreading gossip, rumors, and innuendos about co-workers or others;
- Submitting unnecessary mail attachments;
- Transmitting copyrighted materials without permission;
- Use that reflects non-professional image of DIS

2.3. E-mail Storage

DIS employees should move important information from E-mail message files to shared folders and drives to ensure proper backup. Messages no longer needed must be periodically purged from personal storage areas. Technical support staff will monitor storage usage and advise when limits are reached and purging is required. Additionally, any e-mail created that is substantive must be retained according to the **Arkansas Records Retention Schedule**. See also the DIS **Records Retention Standard**.

3. Internet

3.1. Purpose of Internet Access

The Internet provides a wealth of information useful for educational purposes. With Internet access DIS employees can utilize the many research and resource tools available online. These tools can aid in preparing reports or projects required by DIS.

All DIS employees may access the Internet to benefit DIS programs and services. The Director may restrict employees to allow such use only for specific circumstances or tasks.

3.2. Appropriate Use of Web Access

Employees are responsible for making sure they use this access correctly and wisely. Staff should not allow Internet use to interfere with their job duties. Generally, such acceptable uses include:

- Accessing and distributing information that is in direct support of the business of DIS;
- Providing and simplifying communications with other state agencies, school districts and citizens of Arkansas;
- Professional development or to remain current on topics of interest to DIS;
- Announcement of new laws, rules, or regulations; and
- Encouraging collaborative projects and sharing of resources.
- Brief and occasional personal use of the Internet is acceptable as long as it is not excessive or inappropriate, does not violate any of the prohibitions in Sections 1.4 and 3.3.

3.3. Inappropriate use of web access includes, but is not limited to:

- Viewing, downloading or sending pornographic or other obscene materials;
- Playing or downloading games;
- Visiting and/or participating in social media in an excessive manner that is not designed for professional interactions specifically related to one's job;
- Browsing the Web for inordinate amounts of time;
- Otherwise endangering productivity of DIS;
- Purposes which violates a federal or Arkansas law;
- Dissemination or printing copyrighted materials (including articles and software) in violation of copyright laws
- Using the DIS network or web access to access personal e-mail or instant messaging accounts;
- Downloading radio, video or music transmissions excessively from Internet sites that are not designed for professional interactions specifically related to one's job;

- Gambling or participating in fantasy sports leagues; or
- Streaming non work-related media such as music or video.

4. Appropriate Network Use and User Accounts Guidelines

Use of the state's Internet connection and e-mail resources is a privilege and it is expected that all DIS employees abide by acceptable user guidelines. Appropriate guidelines for users include:

- Only access those computer accounts which have been authorized for their use;
- Authorization to connect devices to protected networks, such as networks including but not limited to FTI and PCI data must be approved by the DIS CSO and the SCO of the controlling agency;
- Only use accounts for authorized purposes. This policy shall not prevent informal communication, but accounts must not be used for private consulting or personal gain;
- Understand that network administrators may review files and communications to maintain system integrity and ensure that users are using the system responsibly. DIS employees should not expect files and documents to remain private;
- Maximize, to the extent possible, the use of the technologies covered under the DIS policy to reduce the cost of postage, letters, reports, etc.;
- Protect assigned USER ID and system passwords from unauthorized use;
- Assume responsibility for any charges associated with billable services unless appropriate authorization has been obtained; and
- Take note that electronic records including, but not limited to, e-mail, documents, meeting records and presentations are public records subject to the Freedom of Information Act (FOIA), Personal Privacy Protection Laws, the Arkansas Records Retention Schedule, and discovery proceedings in legal actions.

5. Copyright Guidelines

5.1. Purpose of Software Availability

DIS provides utility and application software that enhances the efficiency and productivity of its employees. DIS employees must honor copyright laws regarding protected commercial software used at DIS.

5.2. Compliance with Copyright Laws

- Copyright laws do not allow a person to store copies of a program on multiple machines, distribute copies to others via disks or Internet, or to alter the content of the software, unless permission has been granted under the license agreement.
- Unauthorized use of copyrighted materials is considered copyright infringement.
- Any user that copies and distributes software in any form for any purpose should do so only on the authority of the user's immediate supervisor.
- Each user is responsible for observing all local, state and federal laws, especially in regard to copyrighting. DIS will not be responsible for the cost of any legal action taken against any user that violates such laws regardless of the situation or the intent or purpose of the user.
- Any copyright questions or issues an employee may have shall be directed to the DIS General Counsel.

6. Social Media

6.1. Definitions

Social Media is primarily Internet and mobile-based tools for sharing and discussing information. The term most often refers to activities that integrate technology, telecommunications and social interaction. Examples include but are not limited to the following:

- Forums
- Weblogs (blogs, vlogs, microblogs, presence applications)
- Wikis
- Taggings
- Social Communication Sites
- Podcasts
- Videos (video, vlogs, livecasting)
- Real-Time Web Communications (instant messaging, video chat)

6.2. Communicating on Behalf of DIS

Some employees routinely engage, or may be specifically delegated to engage, in communications through social media as a part of their job. This is particularly true with respect to social media sponsored by professional organizations through which an employee is a member or affiliated with as a result of their work.

If the communication involves the discussion of policy, budget issues, technology issues, legislative affairs, legal matters or litigation, or the business before any board or commission, the communication should also be reviewed and approved by the Director.

- Always identify yourself and your position with DIS.
- Comments must not contain political views, commercial endorsements or recommendations, or discriminatory, racist, offensive, obscene, inflammatory, unlawful or otherwise objectionable statements, language or content.
- Comment only in areas of your expertise or job responsibility. Refer matters to others within DIS as necessary.
- Retain social media comment/communication under the **Arkansas Records Retention Schedule** to the same extent as other communications. It depends on the nature of the communication as to its classification.
- Comply with state and federal laws and DIS policies, including those dealing with confidential information, privacy, ethics and employee conduct.
- Be polite, respectful and professional.
- Be honest and factual. If you inadvertently provide inaccurate information, correct it as soon as possible.
- Do not violate copyright or trademark laws. Be respectful of proprietary information.
- Be respectful of the privacy of the citizens we serve.
- Remember that all employees are responsible for what they write.

6.3. Personal Use of Social Media and Its Impact on Work

DIS respects the rights of its employees to use personal websites, blogs and other forms of social media as a means of self-expression. However, certain conduct standards and rules apply even with respect to such off-duty conduct:

- Do not post your state e-mail address or telephone number on a personal blog or website.
- Be respectful of co-workers and their privacy. Online conduct can violate the agency's anti-harassment policy. Disclosures of information about co-workers or direct reports can violate confidentiality provisions of various state and federal laws, including but not limited to the FOIA and the Health Insurance Portability and Accountability Act (HIPAA).
- Do not engage in political activity during work time.
- Be careful with respect to the disclosure of any information gained as a result of your employment with DIS. You will be responsible for the release of any confidential information obtained as a result of your employment. Do not publish or report on conversations that are meant to be pre-decisional or internal to DIS.
- Be aware that there are criminal and/or civil penalties for such things as defamation (libel or slander), copyright or trademark infringement, invasion of privacy and harassment.
- If you identify yourself as a DIS employee, ensure that your profile and related content (even if it is of a personal and not an official nature) is consistent with the presentation of yourself as a professional.

7. Use of Personal Electronic Devices at Work

Personal mobile devices that connect to the DIS network will be governed by DIS Security Policies, the **Encryption of Portable Data Policy** and **Mobile Device Management MDM Bring Your Own Device BYOD Policy**.

8. Compliance

All agency employees are responsible for complying with the policy. Penalties for non-compliance include but are not limited as follows:

- Suspension or usage restrictions of Internet service and e-mail/messaging services, or authority to communicate for work purposes using social media;
- Disciplinary measures, including discharge; and
- Initiation of criminal or civil action, if appropriate.

9. Related Documentation

Software and Hardware Policy
Mobile Device Management MDM Standard and Procedure

10.Revision History

This policy shall be subject to periodic review according to the State Cybersecurity Office (SCSO) Regulatory Settings spreadsheet to ensure relevancy.

Date	Description of Change	Reviewer
5/21/2025	Updated for format and policy alignment	Gary Vance, Chief Information Security Officer