MISSOURI DEPARTMENT OF TRANSPORTATION
PERSONNEL POLICY MANUAL

POLICY TITLE: Communications and Information Systems
NUMBER: 2503
CHAPTER TITLE: Employee Conduct

EFFECTIVE DATE: June 1, 2025
PRIOR EFFECTIVE DATE: April 1, 2023

POLICY STATEMENT

Information technology resources and equipment are provided to employees and others to conduct department business. Improper use of the department's information technology resources or equipment can result in loss of productivity, create legal liability, cause the loss or destruction of records, and create unacceptable positions for employees and the department. Frequent personal use exposes the department to multiple risks of viruses, hacking, loss of productivity, and the possible abuse of licensing agreements. This policy establishes rules governing the use, protection, and security of the department's information technology resources and equipment. This policy covers employees and others (e.g., contractors and consultants) who are granted access to department resources. Non-compliance with this policy may result in disciplinary action, up to and including termination.

SYSTEM USERS DO NOT HAVE AN EXPECTATION OF PRIVACY IN ANYTHING THEY CREATE, STORE, ACCESS, SEND, OR RECEIVE ON INFORMATION TECHNOLOGY RESOURCES AND EQUIPMENT, EVEN FOR LIMITED PERSONAL USE AS ALLOWED UNDER THIS POLICY.

DEPARTMENT MEETINGS ARE SUBJECT TO BEING RECORDED BY AUDIO AND VIDEO AT ANY TIME WITH ADVANCE NOTICE AND APPROVAL AS OUTLINED IN PERSONNEL POLICY 2500, "STANDARD RULES OF CONDUCT."

DEPARTMENT VEHICLES MAY BE EQUIPPED WITH A TELEMATIC DEVICE CAPABLE OF MONITORING EQUIPMENT DIAGNOSTICS, VEHICLE USAGE, OCCUPANT BEHAVIOR, POTENTIAL COLLISIONS, AND ACCIDENT AND LIABILITY INFORMATION. VEHICLE OPERATORS AND OCCUPANTS DO NOT HAVE AN EXPECTATION OF PRIVACY IN THEIR ACTIONS, OPERATIONS, LOCATIONS, OR BEHAVIORS WHILE IN A DEPARTMENT VEHICLE.

DEFINITIONS

Information Technology Resources: Networks, workstations, servers, computers, all supporting software, telephones, mobile devices, printers, fax machines, and copiers.

Information Technology Equipment: Hardware such as personal computers, notebook computers, hand-held electronic communication devices, mobile devices, and software, as well as operating systems and software required to perform activities such as word processing, statistical analysis, graphics, and computer aided drafting.

Personal Use: The use of any department information technology resources or equipment that is not for the purpose of conducting department business or making changes in work-related overnight and/or travel accommodations (including notification of family members) due to changes in work schedule.

General Correspondence: Documents and written communications, including text messages, of a general nature that were created or received pursuant to law, or in connection with the transaction of official business, which are not included in another records series.

Transitory Records: Drafts or other documents having short-term value and which are not an integral part of administrative or operational records file; not required to sustain administrative or operational functions; not regularly filed under a standard records classification system; not required to meet statutory obligations; **and** recorded only for the time required for completion of actions.

Artificial Intelligence: The theory and development of computer systems able to perform tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages.

PROVISIONS / REQUIREMENTS

1. District engineers and division leaders/state engineers are accountable and responsible for the dissemination and administration of this policy.

2. Employees and others granted access to information technology resources and equipment are authorized to access only the department information required to perform their jobs. In accessing and using department information, employees and other authorized users must ensure its protection and privacy by refraining from distributing or forwarding information to inappropriate parties inside or outside the department. Access to department information the employee or other authorized user does not need to perform their job is strictly prohibited.

3. Employees are prohibited from sending electronic communications to all department employees (e.g., via the USERS email distribution group) without authorization to do so. If an employee has a request to share a message with a broader audience than their access allows, this request should be discussed with the employee's immediate supervisor.

4. All users must safeguard department information. Employees and other authorized users should be aware that many electronic department documents and written communications, including text messages, might be subject to disclosure under the Missouri Open Records Act (Sunshine Law). A broader range of documents would be subject to disclosure in response to a subpoena issued as a part of a lawsuit or a criminal investigation. Therefore, all users must treat electronic documents and written communications, including text messages, with the same level of care and attention, both in production and storage, as are accorded printed documents and communications.

a. It is the employee's responsibility to evaluate each record's content to determine if it is transitory in nature or whether it is a business-related record. If records are determined to be business-related the employee must ensure the record is stored in the appropriate location where retention is established and not only on the mobile device. Employees are responsible for consulting with their supervisor and Human Resources to verify whether documents are transitory in nature.

b. Text messages and other electronic records are not to be deleted from a mobile device unless the record is determined to be transitory in nature and there is no applicable retention hold in effect, or the record has been replicated to an appropriate location.

c. It is the responsibility of the employee to ensure business records stored only on mobile devices are properly retained or copied to an authorized location such as Microsoft OneDrive, Teams, or SharePoint.

Employees are prohibited from engaging in any activity or using any application or system that circumvents the retention of documents and written communications, including text messages.

5. Access to information technology resources will be immediately deactivated when a department employee or other authorized user terminates employment or rights are withdrawn for any other reason. Anyone attempting to access information after termination will be referred to the appropriate legal authorities for prosecution.

6. All use of state information technology resources or equipment will be audited and monitored and will include all usage, whether performed by the employee during or after work hours. The department reserves the right to review, audit, intercept, access, and disclose all matters on the department's networks, workstations, servers, e-mail, MoDOT provided mobile devices, and internet and intranet systems at any time, with or without user notification.

Employees should not download applications (apps) to MoDOT provided cellular devices to conduct health and wellness, banking, or other personal confidential and sensitive activities, as their information will be subject to these policy provisions, and there is no expectation of privacy.

7. Employees and other authorized users are strictly prohibited from using the department's information technology resources, equipment, and other communications systems in connection with the following activities:

a. Engaging in illegal, fraudulent, or malicious conduct;

b. Working on behalf of organizations with no professional or business affiliation with MoDOT;

c. Operating or supporting a private or personal business with department resources;

d. Creating school, scout, church, or other non-business newsletters/ bulletins, etc.;

e. Gambling or maintaining betting pools;

f. Accessing, sending, receiving, or storing offensive, sexually explicit, pornographic, or defamatory material;

g. Purposely annoying or harassing other individuals;

h. Creating, sending, or forwarding uninvited e-mail or other electronic communications of a personal nature;

i. Monitoring or intercepting the files or electronic communications of employees or third parties;

j. Forwarding, copying, printing, distributing, or using information in e-mail or other electronic communications for which they are not the intended recipient;

k. Obtaining unauthorized access to any computer system;

l. Using another individual's account or identity without explicit authorization;

m. Attempting to test, circumvent, or defeat security or auditing systems of MoDOT;

n. Distributing or storing chain letters, jokes, solicitations, offers to buy or sell goods, or other non-business material of a trivial or frivolous nature;

o. Incurring charges on MoDOT mobile devices, and telephones for personal business/information unless approved by the employee's supervisor; or

p. Using facsimile machines, department equipment, and supplies for printing, copying and/or distributing personal information, with the exception that **limited** personal use will be allowed in relation to the Medical Plan, Cafeteria Plan, Retirement Plan, and other department-related benefit programs.

This list provides examples of prohibited activities. It should not be considered all-inclusive.

8. All employees will occasionally need to use the internet and/or intranet to access information relevant to their jobs. Abuse or misuse of this access can result in the access being removed for individual employees or users at the discretion of district engineers and division leaders/state engineers who are accountable and responsible for the dissemination and administration of this policy.

9. **Limited** personal use of the internet/intranet <u>before work, after work, or during lunch break</u> is permissible as long as it does not violate any of the other sections of this policy. The use should be infrequent and must not:

a. Interfere with the work of the authorized user or their co-workers;

b. Consume system resources or storage capacity on an ongoing basis, such as when streaming Internet radio;

c. Incur additional costs for access;

d. Involve large file transfers or otherwise deplete system resources available for business purposes;

e. Be used for hosting personal HTTP, FTP, e-mail servers, or any type of internet/intranet service; or

f. Use peer-to-peer file sharing software.

10. Use of personal pictures (for example, .gif or .jpeg files) for screen savers and wallpaper is permissible as long as they are work appropriate and do not violate any of the other sections of this policy.

11. Signature blocks and profile pictures used in department accounts or programs visible to others (for example, email, instant messaging, virtual meetings, training, etc.) should portray a professional image and not contain other individuals or identifiable backgrounds that are not related to department business or that otherwise violate any provisions of this or other department policies. Please refer to the [E-mail Signature Block Guidance Document](#) for further information.

12. Backgrounds visible to others during virtual meetings must be work appropriate and not violate any provisions of this or other department policies.

13. Department e-mail accounts have been provided to users to conduct department business. **Limited** personal use of department e-mail is permissible as long as it does not violate any of the other sections of this policy. Use of any form of e-mail other than a department e-mail account to conduct department business, is strictly prohibited, unless approved by Information Systems (IS) management.

14. Department e-mail accounts and MoDOT provided mobile devices have been provided to users as communication tools. Therefore, emails and text messages shall be retained for five years and six months to be more closely aligned with the recommendation set forth by the Secretary of State for general correspondence. *See Exemptions. Any e-mails (including attachments) and text messages that are deemed to be records subject to retention under a different retention series (due to the nature of their content), shall be treated as an official record and stored in an appropriate location where retention is established.

    *Exemptions E-mail and text message retention for the Commission Secretary's Office is six years to match the terms of appointed Commissioners.

    The Chief Counsel's Office staff will be exempt from automatic deletion since litigation often lasts beyond five years. These steps are necessary to accommodate the length of time a case may be open and to protect legal information that may be stored within e-mails and text messages.

15. Instant messaging software has been provided to users to conduct department business only. Use of any other form of instant messenger to conduct department business, is strictly prohibited, unless approved by IS management.

16. MoDOT-managed Voice Over Internet Protocol (VOIP) software has been provided to users to conduct department business only. Use of any other form of VOIP technology to conduct department business is strictly prohibited.

17. MoDOT business related documents, images, text messages, and files generated, transmitted, or stored on a MoDOT mobile device must be retained consistent with MoDOT's document retention schedule and stored in an appropriate location where retention is established.

18. Employees are prohibited from using their personal telephone, mobile devices, or other computer equipment to conduct department business except for emergency situations when no other equipment is available, to access cloud applications (such as MoDOT email and desktop virtualization), and the periodic use of mobile devices for security validations for IS systems and applications.

19. State laws, licensing agreements with vendors, federal laws pertaining to software piracy, and department standards govern the procurement of hardware and software. Violation of laws and agreements can expose the department to legal and financial liability. Departing from standard configurations can jeopardize system performance, cause security breaches, and inhibit the department from rapidly responding to security and virus issues. Individuals may not set up workstations or network devices that do not conform to department standards and operate them on MoDOT's network.

20. Only authorized IS personnel may purchase hardware or software for workstations and network components. In accordance with state statute, all purchases will be through the Office of Administration. Only authorized IS personnel and contractors operating under their supervision may install software or add hardware components to MoDOT networks and facilities.

21. Remote or other access methods may only be established by authorized IS personnel. Unauthorized hardware may not be connected to the network, or software installed on your computer, that allows remote access.

22. Wireless access points for connecting to MoDOT's network may only be established by authorized IS personnel. The relaying, retransmission, or any other interception of radio signals used for wireless access to MoDOT's network is prohibited.

23. Software may not be transferred to any other department, vendor, or home system without approval of personnel authorized to purchase and install hardware.

24. Software may not be downloaded from the internet for trials, purchase, or any other use unless approved by personnel authorized to purchase and install software.

25. All users of MoDOT computing resources must comply with IS Division policies, standards, and guidelines.

Artificial Intelligence (AI)

Applies to all employees and contractors of MoDOT who use or interact with MoDOT or Office of Administration (OA) approved AI systems, including, but not limited to, approved generative AI, machine learning, Large Language Models (LLMs), plugins, enabled AI tools,

and any other circumstance in which AI can be utilized at MoDOT. The use of unapproved, open AI systems (such as ChatGPT, Bing Chat, and other publicly available AI systems) for work-related purposes is prohibited. Open AI systems such as these capture data that is entered into it and then uses that data for training their systems to respond to all users of the system, which is the equivalent of publishing information onto a public website, which is a violation of MoDOT Policy.

Employees inputting data and information into an AI Tool are prohibited from disclosing confidential data or information belonging to MoDOT or MoDOT's partners. The input of confidential or sensitive information could result in the disclosure of such information to third parties. Employees must comply with MoDOT's policies concerning data and record retention, and the proper storage, handling and sharing of sensitive information.

1. Employees who use a large language model (LLM) or generative artificial intelligence (GAI) tools in the writing of a deliverable, production of images or graphical elements of the deliverable, or in the collection and analysis of data must be transparent in disclosing how the AI tool was used and which tool was used. Employees are fully responsible for the content of their deliverables, even those parts produced by an AI tool, and are thus liable for any breach of publication ethics. Specifically, employees should:

   a. Be prepared to disclose the use of language models if questioned, including which model was used and for what purpose.

   b. Verify the accuracy, validity, and appropriateness of the content and any citations generated by language models and correct any errors or inconsistencies.

   c. Document sources used to generate content and citations, including those generated by language models. Double-check citations to ensure they are accurate, unbiased, and properly referenced.

   d. Be conscious of the potential for plagiarism where the AI tool may have reproduced substantial text from other sources. Check the original sources to be sure someone else's work is not being plagiarized conducting thorough testing and validation to ensure the safety, reliability, and fairness of the deliverables.

   e. Acknowledge the limitations of language models in the deliverables, including the potential for bias, errors, and gaps in knowledge. Note that AI bots such as ChatGPT should not be listed as an author on deliverables.

   f. Prior to publishing, employees must receive written approval from a supervisor or division leader.

2. The AI Work Group, CCO and HR will conduct periodic reviews of this policy to ensure adherence to this policy, identify any emerging risks and updates to the policy as necessary.

3. Employees are expected to contact their supervisor or HR immediately if they become aware of:

   a. A possible violation of this policy

   b. A breach of data privacy or security

c. A circumstance where an AI Tool is generating output which is misleading, offensive, discriminatory or which causes an employee to have other concerns, or which violates any other existing MoDOT policy.

d. An employee is using AI tools for non-work-related purposes during working hours.

4. Violations of this policy may result in disciplinary action, up to and including termination.

Ashley Halford
Human Resources Director

CROSS REFERENCES
Personnel Policy 0520, "Personnel Files and Employee Records"
Personnel Policy 2500, "Standard Rules of Conduct"
MoDOT's Retention Schedule
E-mail Signature Block Guidance Document
Information Systems Policies