| *P.O. 1109 MDT, Internet/Intranet, and Mass Notifications* | | | |
|---|---|---|---|
| Effective From: | 05-14-2020 | Effective To: | Current |

## *A. P.O. 1109 - MDT, Internet/Intranet, and Mass Notifications*

1. MOBILE DATA TERMINALS
   - i) Equipment
     - a) At the start of each shift, officers shall check the mobile data terminal while completing the regular vehicle equipment checks. Officers shall log onto the assigned mobile data terminal and remain active on the system for the duration of their tour-of-duty. Any problems and/or damage to any mobile data terminal shall be immediately reported to the Information Technology Services help desk.
     - b) Officers shall be responsible for any damage to the mobile data terminal assigned to them.
     - c) The operating temperature of a mobile data terminal is normally between 50 and 85 degrees Fahrenheit. During periods of extreme hot or cold weather, the vehicle should be run for at least ten (10) minutes with the proper environmental controls set before attempting to turn on the computer.
     - d) Officers must log-off and properly shut down the computer at the end of their tour-of-duty. If weather conditions are extreme, it is recommended that the officer disconnect the mobile data terminal and store it in a temperature-controlled environment.
     - e) An officer should utilize the mobile data terminal at a minimum while operating a vehicle in motion and should do so in a safe and cautious manner.
   - ii) Information Access
     - a) All inquiries made using a mobile data terminal are subject to NCIC, state, and Department guidelines.
   - iii) Audible Alarms
     - a) The audible alarm setting on all computers shall be left on. No officer shall in any way tamper with the audible alarm function for incoming messages, announcements and alarms.
   - iv) Motor Vehicle Stops, Driving While Suspended Violations and "Hit" responses
     - a) Officers are encouraged to query as many registration numbers as possible during a tour-of-duty. Probable cause to stop shall be established prior to initiating a stop.
     - b) A motor vehicle query may be made without any prior suspicion of wrongdoing. As a result of information received, the officer may make a valid stop for problems related to the vehicle itself and/or the owner's driver's license.

c) The following must precede stops based upon license plate inquiries that indicate the registered owner's license is suspended:
    1) After receiving the suspension information, the officer must attempt to verify that the driver of the vehicle to be stopped generally matches the sex and age description of the registered owner listed on the response.
    2) When the information reveals a problem with the vehicle itself, a valid stop is proper without any further corroboration.
    3) In the event an inquiry results in a NCIC or state CCH "Hit" response, all online system users will automatically be notified via alarm. All "Hits" shall be confirmed through the communications centers prior to taking action based solely upon this response.

2. ELECTRONIC MESSAGING, USE OF THE INTERNET/INTRANET, ELECTRONIC MAIL, MOBILE DATA TERMINALS AND CELLULAR TELEPHONES
    i) This order is applicable to all Department of Public Safety personnel including full time, part time, temporary and contract employees, whether commissioned or non-commissioned personnel, within the Office of State Police. It shall also apply to any consultants, student interns or volunteers which may have an approved need to utilize any of the Department's electronic messaging systems. For the remainder of this policy the persons listed above shall be referred to as "employees."
    ii) This order requires all employees to abide by all state and federal laws pertaining to the use of Department computers, the dissemination or acquisition of electronic information, the use of Mobile Data Terminals and the use of cellular telephones.
3. COMPUTER COMPLIANCE PROVISIONS
    i) The following information contains the provisions limiting the use of Department computers, and limitations on electronic mail, Internet, and systems while operating Department computers.
    ii) The Department licenses the use of its computer software from a variety of outside companies. The Department does not own this software and unless authorized by the software developer, does not have the right to reproduce the software or any of its related documentation. Therefore, unauthorized duplication of software is prohibited.
    iii) With regard to use on Local Area Network (LAN), Wide Area Network (WAN), or multiple computers or terminals, employees shall use the software in accordance with the license agreement.
    iv) According to the US Copyright Law, illegal reproduction of software can be subject to civil damages of $50,000 or more and criminal penalties, including fines and imprisonment.
    v) Departmental hardware and software use is strictly for completing matters pertaining to the Department's mission. Personal use of hardware, software, or the data retrieved from the state files is prohibited.

vi) Uses of Department computer equipment, electronic mail, the Internet, and Department systems that interfere with normal business activities, involve solicitation, are associated with any for-profit business activities, or could potentially embarrass the state or the Department, are strictly forbidden.

vii) Department computer equipment, electronic mail, the Internet, and Department systems will not be used for operating a business for personal gain, searching for jobs, sending chain letters, or soliciting money for religious, political, or any other cause.

viii) Electronic messages shall not contain offensive or harassing statements including disparagement of others based on their race, color, religion, marital status, creed, political affiliation, national origin, sex, sexual orientation, handicap or age.

ix) Department computer equipment, electronic mail or electronic networks shall not be used to send or solicit sexually-oriented messages, images, or materials.

x) Electronic messages shall not contain inflammatory statements which might incite violence or describe or promote the use of weapons or devices associated with terrorist activities.

xi) Department computer equipment, electronic mail or electronic networks shall not be used to disseminate or print copyrighted material (including articles and software) in violation of copyright laws.

xii) Employees shall not provide access to confidential information by use of Internet or e-mail. All use of the Internet and e-mail must be done in compliance with the rules and regulations that apply to such information.

xiii) Employees shall not use an account (Internet, electronic mail or bulletin board systems), signature line or password other than their own.

xiv) Employees shall take all reasonable means to prevent the inadvertent dissemination of anyone else's information via any means, electronic or otherwise.

xv) The Department, learning of any violation of this agreement, will discipline offending employees as appropriate under the circumstances, and in accordance with established and applicable law and administrative rules.

xvi) Employees wanting to install personally-acquired software and/or disc, including shareware and freeware, on their state-owned computer equipment, must submit a work order to Information Technology Services, utilizing their chain-of-command. This request may be approved if the employee can show compliance with all copyrights to the software and the software is relevant and necessary to the employee's position. Also, software and disc must be scanned for virus infection before installation.

xvii) No copies of the software used within the Department will be made unless authorized by Information Technology Services.

xviii) No DPS-owned software will be loaned out for use to an individual or other state agency.

xix) Transfers of software from one personal computer to another shall be performed by Information Technology Services.

4. ELECTRONIC MAIL ACCESS
    i) Electronic Mail Storage and Retention
        a) Electronic mail is stored on file servers throughout the Department.
        b) Electronic mail should be retained in accordance with the DPS Records Retention Schedule.
        c) Electronic mail messages and information shall be treated with the same degree of propriety, professionalism, and confidentiality as official written correspondence.
        d) The use of electronic mail is a privilege that is subject to revocation.
    ii) Privacy Expectations, Electronic Files and Electronic Mail
        a) Employees must treat electronic messages and files as a private and direct communication between a sender and a recipient.
        b) Electronic mail and files will not be routinely monitored.
        c) Management reserves the right to review electronic mail messages and files to ensure adherence to this policy. This includes requiring employees to provide passwords to files that have been encrypted or password protected.
        d) Employees do not maintain any right to privacy of electronic mail or files, including personally-owned software approved for loading on Department computers.
    iii) Personal Use of Computer Equipment, Electronic Files and Mail
        a) Employees should utilize electronic files and electronic mail for Department business.
        b) Employees should limit their use of state computer equipment and resources to hours of business.
5. INTERNET ACCESS
    i) As part of the Department's commitment to the utilization of new technologies, many of our employees have access to the Internet. To ensure compliance with the copyright law and to protect ourselves from being victimized by the threat of viruses or hacking into our services, the following is effective:
        a) Access to the Internet will be provided to employees when their job functions dictate a need. Supervisors will determine and document the need for access. Justification will be forwarded through the employee's chain-of-command to Information Technology Services, which is responsible for providing access.
        b) It is the Department's policy to limit Internet access during business hours to official business.
        c) The introduction of viruses or malicious tampering with any computer system is expressly prohibited.
        d) Employees using the Department's account are acting as representatives of the Department. As such, employees should act accordingly so as not to damage the reputation of the organization.

e) Files which are downloaded from the Internet must be scanned with virus detection software before installation or execution. All appropriate precautions should be taken to detect a virus, and if necessary, to prevent its spread.

f) The truth or accuracy of information on the Internet and in e-mail from unknown senders should be considered suspect until confirmed by a separate and reliable source.

g) Employees shall not place any material (copyrighted software, internal correspondence, etc.) on any publicly accessible Internet computer without permission from the Superintendent.

h) Alternate Internet Service Provider connections to the Department's internal network are not permitted unless expressly authorized through Information Technology Services and properly protected by a firewall or other appropriate security device.

i) The Internet does not guarantee the privacy and confidentiality of information. Sensitive material transferred over the Internet may be at risk of detection by a third-party. Employees must exercise caution when transferring such material in any form.

j) Unless otherwise noted, all software on the Internet should be considered copyrighted work. Therefore, employees are prohibited from downloading software and/or modifying any such files without permission from the copyright holder.

k) Any infringing activity by an employee may be the responsibility of the Department. Therefore, this organization may choose to hold the employee liable for their actions.

l) The Department reserves the right to monitor an employee's use of Department equipment or to inspect an employee's assigned computer system for violations of this policy.

6. MASS NOTIFICATION SYSTEMS

i) All mass communications from the Department to a group of employees, whether by electronic mail, mass text notification, or any other system, is confidential unless expressly stated otherwise within the message and regardless of the device upon which the mass communication is received. Such confidential information shall not be disseminated to individuals outside of the Department without proper authority.