UW–Madison Police Department

Policy: 11.5
SUBJECT: COMPUTER USE
EFFECTIVE DATE: 06/01/10
REVISED DATE: 04/17/19; 11/19/19; 07/21/21; 9/21/22; 9/26/23; 10/18/24
REVIEWED DATE: 02/01/17; 11/25/20; 03/03/23 STANDARD: CALEA 11.4.4, 41.3.7

INDEX:

POLICY:

Each employee is expected to protect the integrity of the department's IT resources and to adhere to University and Department rules, regulations, and guidelines for their appropriate use. Each UW–Madison Police Department employee is part of a network of IT users. To maintain the integrity of information technology systems, all employees shall adhere to the guidelines set forth in this policy.

DEFINITIONS:

Computer "hardware" refers to the mechanical, magnetic, electronic, and electrical devices constituting a computer system, such as the CPU, disk drives, keyboard, screen, USB Drives, and cameras/microphones.

Computer "software" refers to the programs used to direct the operation of a computer, as well as documentation giving instructions on how to use those programs.

"Remote Worker" refers to UWPD Employee not at UWPD Headquarters or on UW Madison Campus doing work for UWPD.

PROCEDURE:

11.5.1 COMPUTER USE – GENERAL

A. Computers, software, databases, e-mail accounts, Internet access, and other information technology (IT) resources are tools provided by the Department to employees to support the missions of both the University and the Department, and can be revoked at anytime

B. Department IT staff shall provide training in the use of computers and software required for each position. Employees shall use computer resources in a manner consistent with their training to maintain a system that is secure, reliable, and predictable.

C. Access to University IT resources is a privilege granted to members of this Department to be used for appropriate University and Department related activities. Authorization for the use of IT resources is provided to each employee for their exclusive use and is not permitted to be used by others (i.e., friends, family members, guests).

D. The protection of University IT resources depends heavily on each user's careful handling of the "keys" (accounts, access, and passwords) to these resources, since any account can serve as an entry point for theft, damage, or unauthorized use. These "keys" should be changed frequently and their security protected to prevent unauthorized intrusions into the network. Employees are responsible for the security of the "keys" provided to them.

E. Department members are responsible for their own network account, regardless of who actually uses it; therefore, they are responsible for logging off the network upon completion of their computer activity.

F. Playing or downloading/configuring any form of interactive software material/game is generally prohibited. If there is a business value to interactive material, it should be checked by the IT Staff and approved by a supervisor.

G. If an employee believes a computer has become infected with a virus, malware, spyware or other malicious code, then the employee is to immediately turn off the computer, disconnect it from the network, notify the OIC. The OIC shall notify the MOC and IT Director. The employee shall not try to remove malicious code unless directed to do so by IT Director. If it is believed a data breech occurred from the malicious code, then it needs to be immediately reported to a supervisor or MOC and the IT Director.

11.5.2 COMPUTER USE

A. Employees shall not obtain or use or attempt to obtain or use any hardware or software resources not assigned to them or without prior approval from the IT Director.

B. Employees shall not alter or intentionally damage University or privately owned software or data or interfere with an authorized user's access.

C. Employees shall not add, delete, or alter the desktop default settings on common workstations.

D. Personnel shall not obtain or use—or attempt to obtain or use—passwords, IP addresses, or other network codes that have not been assigned to them as individuals or authorized for their use as University employees. Persons shall not obtain—or attempt to obtain—unauthorized access to computer accounts, software, files, or any other University IT resources, unless as part of a criminal investigation.

E. UWPD personnel shall abide by all Terms of Service as stipulated by the site or software; this includes, but is not limited to, a prohibition of falsely identifying oneself on a site or sites other than for investigatory purposes, infringing on copyrighted material, and violating the privacy or rights of other users.

F. Employees shall not access profane, obscene, inappropriate, offensive, or illegal material using University IT resources, unless accessing the material is done as part of an official police investigation or for training purposes.

G. In the interest of making the use of University and Department IT resources a natural part of day-to-day work of all members of the University community, incidental personal use is tolerated.

H. IT resources shall not be used for commercial, investment, consultant or extensive non-business use.

I. Department employees shall not use computer resources for making any campaign contribution in support of any person for political office or to influence a vote in any election or referendum.

11.5.3 USE OF SOFTWARE

A. Only properly licensed and IT Director-approved software may be used on Department computers.

B. Prior to the purchase of any new software, users who need specialized software must submit a request to the IT Director documenting the need, the proposed software, the anticipated results, and ongoing support options and costs.

C. The IT Director or designee shall approve and load all software on the system in order to ensure compatibility with the system.

D. Copies of Department-owned software and/or documentation shall be made and distributed in accordance with the software licensing agreement.

E. Only the IT Director or designee may change system-operating files.

F. Software malfunctions should be reported to the IT Director or designee in a timely manner.

G. Demonstration materials obtained from third parties are to be reviewed by the IT Director or designee prior to review or use in any Department computer. USB's received at conferences or trainings are strictly prohibited from being placed on Department computers.

H. Information systems are constantly monitored and data size restrictions have been implemented to help prevent system outages. All data size restrictions are administered by IT and are subject to change without notice. Data that does not need to be kept for business purposes, most notably video and other large files, should be deleted. Data should not be retained longer than required for business purposes or according to open records laws and record retention schedules.

I. Artificial Intelligence (AI) meeting assistant tools are prohibited for UWPD use both for internal and external meetings. All participants must be cognizant of meetings with AI tools in relation to Open Records Laws.

11.5.4 USE OF HARDWARE

A. The addition of peripheral hardware or changes in setup or configuration of multiple-user terminals shall be approved in advance by the IT Director. Use of personally owned flash memory or other portable data storage devices in Department-owned computers is prohibited.

B. Computers are precision instruments and are easily damaged. Special care should be exercised to avoid using food, drink, sprays, physical force, or potentially damaging items in the area of computer equipment. Intentional damage to equipment is prohibited, except in the event destruction is authorized by IT staff.

C. Employees shall report damage, serious problems, and emergency maintenance needs immediately to the IT Director or designee. Routine problems that do not prevent the accomplishment of required work may wait to be addressed during normal business hours.

11.5.5 USE OF MOBILE DATA COMPUTERS

A. Employees shall use the system as specified in training.

B. Police patrol officers and route security officers shall sign on and off the MDC when beginning and ending their shifts, utilizing the radio to notify dispatch of their badge number and what squad they will be riding in for their shift unless exigent circumstances exist.

C. Officers are responsible for making their own status changes from the MDC as these occur.

D. Dispositions shall be completed upon returning to the MDC, unless exigent circumstances exist.

E. All communications are expected to be professional. Communications are subject to open records law and may be monitored by supervisors.

F. Police officers and route security officers assigned to vehicle patrol or a security route should use vehicles equipped with an operational MDC unless exigent circumstances exist.

G. Only personnel specifically authorized and trained may access state and federal databases.

11.5.6 REMOTE CONNECTIONS

A. Prior to remote working the employees supervisor or manager must be satisfied that an alternative work-site is appropriate for UWPD work. The below listed items shall be considered.

a. Remote workers should utilize separate spaces if possible. If a separate room or workspace is not possible, display screens for all UWPD devices must be positioned such that they cannot be readily viewed by unauthorized persons through a window, over a shoulder, or by similar means.
b. Internet line dedication with enough speed and data to perform all given tasks as required. This internet line must include sufficient bandwith at the remote working location that video/audio can be available at any time. Insufficient bandwith may not be used as an excuse for not joining meetings with video and audio on.
c. All department property, electronic or printed, should be securely stored when outside of UWPD buildings.
d. When a remote worker separates from UWPD, the supplied hardware, software, furniture or other information materials must be promptly returned to UWPD upon request from their supervisor/manager.

B. Persons stationed at remote sites shall ensure that their antivirus software and computer are updated on a weekly basis.

C. Remote workers must not use their own mobile computing devices, computers, computer peripherals or computer software for telecommuting business without prior written authorization from the IT Director or designee

D. Remote workers VPN'd to the UWPD network may not remote to any non-UWPD controlled device.
E. Remote controlled sessions of UWPD devices other than by UWPD IT Staff are strictly prohibited.
F. When a remote worker has completed a remote session, the worker must log off and then disconnect, rather than simply disconnecting their UWPD session upon shutdown.
G. Remote workers must have the agency web proxy turned on while VPN'd to UWPD network

11.5.7 COMPUTER USE – PASSWORD PROTOCOLS

A. Each employee is assigned a unique identification (ID) number and is responsible for all business transacted and reading information/messages under their login ID. Any suspected misuse of accounts or passwords must be reported immediately to IT staff.

B. UWPD network passwords shallt be a minimum of twelve characters in length, be memorized, and contain at least one (1) character from three (3) of the following categories
1. Uppercase Letter (A-Z)
2. Lowercase Letter (a-z)
3. Digit (0-9)
4. Special character (@#$%^*&^)

C. Passwords must be kept private, shall not be a dictionary word, and must not contain a common proper name, login ID, email address, initials, or first, middle, or last name. Passwords shall be changed at least every 90 days. The most recent 10 passwords may not be reused.

D. Passwords shall not be shared, stored, transmitted, or transported in an unsecured manner.

E. Personnel should not check or configure options that allow a password to be saved, if the website or program contains CJIS related material.

11.5.8 PHYSICAL SECURITY OF COMPUTERS

A. Access to the computer and server rooms is restricted to authorized personnel.

B. Care should be taken to maintain the physical security of all computer equipment. Possible breaches of physical security (unauthorized access, lost or stolen devices, etc.) should be immediately reported to your immediate supervisor and the IT Director.

11.5.9 INTERNET USAGE AND EMAIL

A. There is no expectation of privacy in using department internal email, external email, internet services or work on State-owned computers. All use of State computers, whether official or personal, is subject to public disclosure laws and can be discoverable in all court proceedings.

B. External Email (Wiscmail) correspondence outside the Department shall contain the employee's contact information including email address, business address and a UWPD phone number.

C. Employees shall not send Criminal Justice Information (CJI) or Other Sensitive or Tactical Information via email unless it is password encrypted utilizing Adobe Acrobat

D. Employees should contact UW-Police IT if they have questions about an email or email attachment. Due to the risk of computer virus attacks and phishing schemes, employees should not open email attachments or click any links from unknown sources. If an employee is notified by the University that they have clicked on a UW Phishing Scheme email or have violated any other University IT Policy they must contact their direct supervisor within 24 hours.

E. Employee Internet use shall not disrupt or interfere with the work of other network users or adversely affect internet service of the department.

F. Employees shall check and respond appropriately to their department internal e-mail(s), assigned VoIP voicemails, or department cell phone voicemail (if assigned) each day they are on duty.

G. Users of University IT resources shall not send electronic messages with the sender's identity forged or send anonymous messages unless this action is part of an investigation.

H. Employees are strictly prohibited from using any personal cellular phone or similar device as a media storage device for the storage or transportation of any UWPD business information.

11.5.10 DEPARTMENT ISSUED CELLULAR PHONES

1. A department issued cell phone shall be carried on the employee's person at all times while on-duty.
2. Employees shall answer calls when available on duty.
3. Employees shall check text and/or voicemail messages while on duty.
4. The device may not be used to conduct personal business while on-duty or off-duty, except for brief personal communications (ex. Informing family member of extended hours).
5. Employees may use a department issued cell phone to communicate with other personnel in situations where the use of radio communications is either impracticable or not feasible. Cell phones should not be used as a substitute for, as a way to avoid, or in lieu of, regular radio communications.
6. Officers should only connect their work phone to their assigned squad to prevent crossovers.
7. While driving a motor vehicle and using a cellular phone, only hands-free operation should be used.
8. Employees shall not text and drive.
9. Text messages on a work device shall not be deleted without supervisor approval for records retention reasons, unless previously preserved for evidentiary reasons.
10. Use of department issued cell phones to harass, threaten, coerce or otherwise engage in inappropriate conduct with any third party is prohibited. Any officer having knowledge of such conduct shall promptly notify a supervisor.
11. While on duty, the device shall be in the control of the person assigned the device, a supervisor, or IT at all times. While off-duty, the department owned cell phone shall either be in the control of the person assigned the device, or secured in a known location that prohibits non-authorized access to the device.
12. Only authorized applications are allowed on the cell phone. Employees shall not install unauthorized applications without pre-approval from IT
13. Conversations and text messages on cellular devices are not considered to be secure forms of communication and consideration should be given prior to engaging in such conversations.
14. There is no expectation of privacy on the device.
15. All communications and data are subject to open records laws.
16. Employees shall not bypass any security measure put in place by the Agency Mobile Device Manager (MDM)
17. Employees shall ensure locations services are always enabled on the Blackberry application.

18. Department established passcodes, setup features, and branding shall not be altered.
19. The department shall issue employees case and screen protectors for department issued cell phones. Employees shall use the case and screen protectors at all times.
20. If a cell phone is damaged and/or not working, the employee is responsible for contacting IT for support, and notifying their supervisor of the status of the phone.
21. The cell phone should have sufficient charge to remain operational during an employee's shift.
22. Charging stations shall be available in the police department and in the squad cars.
23. Devices belonging to the department shall not be assigned a name containing any type of indication that the phone is owned or operated by a Law Enforcement Agency.
24. Agency phones with hot-spotting capabilities shall not have a password that is any type of indication that the phone is owned or operated by a Law Enforcement Agency.
25. Officers shall get permission from a Supervisor to delete pictures, videos, etc. that were captured from the department issued cell phone after proof that the text has been preserved in the appropriate manner. Permission nor preservation is necessary for SPAM or sales texts.