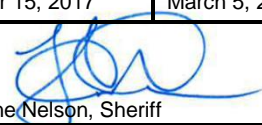




DESCHUTES COUNTY SHERIFF'S OFFICE

Policy Title: Computer, E-mail and Mobile Computing Device Use	Effective Date: October 15, 2014	Policy Number: 4.31	
Accreditation Reference: 1.5.9	Review Date: October 15, 2017	Supercedes: March 5, 2014	Pages: 5
Attachments:	 L. Shane Nelson, Sheriff		

I. PURPOSE

It is the policy of the Deschutes County Sheriff's Office to ensure that Sheriff's Office Computer Resources are used appropriately and the use is consistent with Oregon Public Records and Government Standards and Practices laws.

All agency personnel with access to FBI Criminal Justice Information (CJI), or any system with stored FBI CJI, have a duty to protect the system and related systems from physical and environmental damage and are responsible for correct use, operation, care and maintenance of the information.

II. DEFINITIONS

CJI means Criminal Justice Information.

IT is Information Technology.

FBI means the Federal Bureau of Investigation.

MCD are Mobile Computing Devices. Mobile Computing Devices include laptop computers and cell phones with data access capabilities including smart phones, iPods, tablet PCs, Mobile Data Terminals (MDTs) and other portable electronic computer equipment.

Sheriff's Office Computer Resources include all electronic devices, such as computers, hardware, software, printers, laptops, mobile computing devices, electronic mail (e-mail), internet, and intranet.

III. POLICY

A. General

Except as outlined below, Deschutes County Sheriff's Office computer equipment, including without limitation, hardware, printers, laptops, mobile computing devices, software and other electronic information technology (herein collectively "computer resources") are to be used only for Sheriff's Office business.

The Sheriff's Office may access, enter and inspect Sheriff's Office property assigned to individual employees at any time without notice, including, but not limited to, computer hard drives, software, files, and e-mail.

Sheriff's Office employees' use of computer resources must comply with any and all service or contractual agreements with commercial service providers.

Computer resources are provided and shall be used to conduct Sheriff's Office business. The Sheriff's Office encourages authorized employees to use computer resources as communications, business and research tools when doing so in an official capacity.

Although information contained on Sheriff's Office computer resources may be considered public records, each employee has the responsibility to ensure that the employee's data is adequately protected against unauthorized access by complying with the access controls and other security measures provided by the Sheriff's Office.

Each employee should take prudent and reasonable steps to limit access to that employee's accounts and passwords. An employee's passwords and accounts must remain confidential and should be changed frequently. When changing a password, common, personally related words, such as family member or pet names, should be avoided.

B. Sheriff's Office Records

Unless otherwise specified by written agreement, all Sheriff's Office computer resources are Sheriff's Office records and therefore Sheriff's Office property.

The Sheriff's Office retains the discretion to assert any applicable privileges and objections if a public records request or discovery request is made for any Sheriff's Office e-mail or other information contained in the Sheriff's Office computer resources. An employee may request the Sheriff's Office assert a privilege or objection under the Public Records law. The Sheriff, in consultation with Legal Counsel, will make a final determination on whether to assert the privilege or objection requested.

Personal messages, as well as unsolicited messages and advertisements (spam), are not public records under the retention/disposition aspect of the law but may be accessible to the public under the access portion of the law (ORS 192.410(4)).

In addition, civil suits involving Deschutes County may result in a discovery request and production of your e-mail.

All use of computer resources shall comply with all federal and state confidentiality laws including, but not limited to, the Health Information Portability and Accountability Act of 1996 ("HIPAA"), and with all Sheriff's Office policies regarding confidentiality.

C. Prudent Exercise of Judgment

Employees shall represent the Sheriff's Office's best interests, with a prudent exercise of judgment in the use of Sheriff's Office computer resources. Employees **shall not** visit pornographic sites or write comments in public forums, such as chat rooms, newsgroups and mailing lists, except in the performance of an authorized law enforcement function, and only with the specific consent of the Sheriff or his designee.

When logged in from a site that is identifiable with the Sheriff's Office, employees are prohibited from any communications or activities that are in any way derogatory to the agency or members of the agency.

The Sheriff's Office recognizes each member's right to freedom of speech. However, prior approval from the Sheriff is required if, whether on duty or off duty, an employee decides to make a statement to the public or the media that is in any way derogatory of the agency or its employees. See Sheriff's Office Policy 1.02 Sheriff's Office Standards, Section VIII, A, Conduct Toward the Agency.

Employees shall respect the rights of others. Employees shall not copy or distribute any copyrighted material found on the Internet. Employees are to treat all material as copyrighted, unless the author has given his permission for the material to be redistributed.

All persons accessing computer resources from remote locations are required to have virus checking software installed on the computer equipment used to access the computer resources. The virus checking software must be operational and must be of the latest release.

D. E-mail and Other Electronic Message Use

1. Case-Related Requirement

Case-related e-mails will be printed and filed with the case report. See Sheriff's Office Policy 4.41 Incident Reports and Forms, section IV, A.

2. Professional Use; No Expectation of Privacy

E-mail should be used as a tool only by Sheriff's Office employees or other users authorized by the Sheriff for Sheriff's Office business. E-mail and other electronic messages shall have reasonable communicative purpose and must be professional and business-like.

Users should not expect privacy, but observe courtesy and good security practices. There are a variety of ways an e-mail communication can be disclosed to people other than the intended recipient. The Sheriff's Office shall not be responsible for Internet or e-mail communications that are misdirected or disclosed to third parties due to human or system error or for those that are intercepted by unauthorized individuals.

No communications shall be used to harass, annoy or alarm any recipient or third party. The messages shall not contain language or symbols that would be considered offensive or obscene to a reasonable person. The content shall not bring discredit to any public safety employee, public agency, or to a member of the public.

3. Employer Right to Monitor, Access and Disclose

The Sheriff's Office has the right to monitor, access, and disclose the usage of any Sheriff's Office computer resources. E-mails sent to or from Sheriff's Office computer resources are public records, whether in printed or electronic form, and are subject to the disclosure and inspection provisions of ORS 192 as it currently exists or may from time to time be amended.

E-mail messages may be accessed and reviewed at any time by the Sheriff or his designee, the Information Technology (IT) Manager or Sheriff's Office Legal Counsel; they may also be accessed and reviewed by computer support staff for the limited purpose of providing support services.

4. Retention of Electronic Information

E-mails will be retained for 10 years through the Deschutes County Vaulting System. E-mails are vaulted after approximately 24 hours in the inbox. Employees shall leave e-mails in the inbox until vaulted. After e-mails have been vaulted, employees may delete or move e-mails to folders.

E-mails that are public records shall be retained. Examples of messages sent by e-mail that typically are public records include policies and directives, correspondence related to official business, work schedules or assignments, agendas and meeting minutes, document drafts circulated for comment or approval, documents pertaining to business transactions, and final reports or recommendations.

E-mail, intranet messages and downloaded files shall be retained and destroyed in accordance with retention schedules issued by the Oregon Secretary of State, Archives Division. Records may be retained either in hard copy or electronic format. If a hard copy of the e-mail message or downloaded file is printed, then the electronic version may be deleted. One version should be kept according to the applicable retention schedule and subject to the Oregon Secretary of State, Archives Division.

5. MDT Personal Use

MDT messages used for personal communication are allowed as long as messages are kept brief and professional. All MDT messages are public record.

E. Acceptable Work-Related Internet Use

Acceptable uses of the Internet include, but are not limited to, communication or Internet activity that is in direct support of Sheriff's Office business.

Examples of acceptable Sheriff's Office use of the Internet:

1. Communication for Sheriff's Office purposes;
2. Communication for job-related professional development or to increase knowledge of issues in a field of knowledge; or

3. The use of worldwide webs or search engines to research work-related topics and/or conduct criminal investigations. During investigations, if a pornographic site must be accessed, a supervisor must be notified.

F. Incidental Personal Use

Limited minor and incidental personal use is permitted during non-work time (lunch, breaks and before and after regular work hours). For the limited purpose of compliance with the State Ethics Law (ORS 244.040), this incidental use is considered part of an employee's compensation package.

Examples of limited minor and incidental personal use:

1. send and receive personal e-mail;
2. view an Internet site to check the price of and purchase an airline ticket; or
3. make an investment in a deferred compensation account.

G. Unacceptable Use of Sheriff's Office Computer Resources

Sheriff's Office employees are strictly prohibited from using Sheriff's Office computer resources in connection with any of the activities described below. This list is illustrative of prohibited activities and is not intended to be all-inclusive. If a prohibition exists in any applicable state or federal law, administrative rule, other administrative procedure or directive established within the Sheriff's Office, it is likewise applicable and incorporated by reference herein. While limited minor and incidental personal use is permitted, such use does not include or permit any prohibited activity.

Examples of prohibited activities:

1. Sensitive and/or confidential information will not be shared via e-mail, MDT, or text message, unless authorized by Sheriff's Office Legal Counsel.
2. Attempting to or circumventing, reducing, or defeating security or auditing systems of Sheriff's Office computer resources or those of any other organization without prior authorization from Sheriff's Office Legal Counsel or the Sheriff's Office IT Manager.
3. Taking any action that attempts to or renders the user's computer equipment unusable or that interferes with another's use of Sheriff's Office computer resources including any activity around the workstation that may result in damage to any Sheriff's Office computer resources.
4. Obtaining unauthorized access to any computer system.
5. Using another individual's password, account or identity without explicit authorization of the individual, unless this is approved by the Sheriff.
6. Providing the employee's own password, access identifiers or other access to Sheriff's Office computer resources, to anyone not authorized by the Sheriff or his designee.
7. Monitoring or intercepting the files or electronic communications of employees or third parties, unless this is approved by the Sheriff or as an authorized use of a particular software program (e.g., calendar management).
8. Except as allowed under any software license and as authorized by the Sheriff's Office IT Division, copying or downloading any software from or onto Sheriff's Office computer resources. **No unauthorized software or hardware is permitted on Sheriff's Office computer resources.** Any commercial software residing on Sheriff's Office computer resources shall be purchased through an authorized vendor or otherwise lawfully obtained. Except as otherwise allowed under the software license obtained by the Sheriff's Office, and except for backup/archival purposes, software owned by the Sheriff's Office or installed on Sheriff's Office computer resources is covered under the copyright laws and shall not be copied, duplicated, or installed on any other computer resource.
9. Soliciting or supporting political or religious causes or beliefs unless otherwise allowed under ORS 260.432 for elected officials.

10. Using Sheriff's Office computer resources in a manner that would constitute or might be construed by a reasonable person to constitute an endorsement of a specific commercial entity.
11. Working on behalf of organizations without any professional or business affiliation with the Sheriff's Office, or working on behalf of organizations with such affiliation but outside of the specific Sheriff's Office business with them.
12. Except as expressly authorized by the Sheriff or his designee, as a matter of Sheriff's Office concern, using Sheriff's Office computer resources to solicit for non-profit or charitable activity.
13. Visiting or viewing pornographic Internet sites, downloading pornographic materials from the Internet, sending or retrieving sexually explicit or objectively offensive messages, cartoons or jokes, ethnic slurs, racial epithets or any other statement or image that might be construed as Harassment (as defined by ORS 166.065, Sheriff's Office Policy 3.60 Harassment/Discrimination in the Work Place or the County's Non-Harassment Policy), disparagement, libel, or discrimination based on age, marital status, sex, race, sexual orientation, national origin, disability, or religious or political beliefs.
14. Using Sheriff's Office computer resources for personal financial gain or the financial gain of the user's family, or for the avoidance of personal financial detriment or the avoidance of personal financial detriment to the user's family.

H. Mobile Computing Devices (MCDs)

Mobile Computing Devices include laptop computers and cell phones with data access capabilities including smart phones, iPods, tablet PCs, and other portable electronic computer equipment.

The Sheriff's Office IT Division will support only those MCDs purchased and owned by the Sheriff's Office. Support for Sheriff's Office owned mobile computing devices includes installation, training, and interfacing to Microsoft calendaring, e-mail, tasks, and notes.

MCDs owned by Sheriff's Office employees will not be supported. Non-Sheriff's Office owned mobile computing devices may **not** be connected in any way to the internal Sheriff's Office secure network. Assistance for non-Sheriff's Office owned mobile computing devices will be limited to providing the configuration parameters necessary to establish a connection to approved Sheriff's Office resources.

Non-Sheriff's Office owned MCDs shall not be authorized to be used to access, process, store, or transmit state or FBI CJI.

The Sheriff's Office IT Division will not assume responsibility for data loss on MCDs. Use of mobile computing devices to connect to Sheriff's Office resources must be approved by the Sheriff.

Mobile computing devices are computing and data storage devices. Mobile computing device users assume all responsibility for securing their mobile computing device and its data in accordance with the Sheriff's Office computer usage policy, the guidelines presented in the County security training, and all federal, state, and local laws to which the data is subject.

I. Enforcement

The Sheriff's Office will investigate any alleged abuses of its computer equipment resources. As part of the investigation, the Sheriff's Office may access the electronic files of its employees.

Although the Sheriff's Office wishes to ensure that the personal information of its employees is protected, in the course of its investigation, the Sheriff's Office may reveal private, employee-related information to other employees.

Employees violating any aspect of this policy may have their access to computer resources restricted and are subject to discipline, up to, and including, termination of employment.