
COMPUTER / CELL PHONE USE, EMAIL AND INTERNET ACCESS

POLICY

It is the policy of the Marin County Sheriff's Office that use of Sheriff's Office computers, computer systems, email, and Internet access while on duty shall only be for purposes relating to achieving the Sheriff's Office mission.

DEFINITIONS

Computer/Computer System – Any electronic device, either connected to a network or standalone that uses a micro processor and is capable of receiving input, storing, and outputting any type of digital data including photographs, text, video, and audio. A computer or computer system includes, but is not limited to, any network or standalone workstation, dumb terminal, laptop or portable computer, mobile data computer (MDC), personal digital assistant (PDA), tablet, smart phone or mobile telephone.

For the purposes of this order, a single-user computer means any computer or computer system that is used exclusively by only one employee.

For the purposes of this order, a multi-user computer means any computer or computer system that is used regularly by two or more employees.

Email – Email is a computer generated message of any kind that is capable of being digitally received or transmitted by a computer or computer system using a connection to another computer or computer system. This connection can be wired or wireless using a computer network infrastructure. Email may have other types of digital files attached, such as photographs and audio or video files, which may be transmitted or received in the same manner. The Sheriff's Office typically uses Microsoft ™ Outlook to send and receive email. Email includes car-to-car messaging using a mobile data system.

Internet – The Internet is the network mechanism used to access the World Wide Web (WWW). The World Wide Web is defined as any digital information source accessed via modem, network (wired or wireless), or other means, from a source external to or apart from the computer or computer network through which the information is sought.

Remote Email – Remote email is a Sheriff's Office email account that can be accessed from a computer or other device outside of the Sheriff's Office secure network. Typically, remote email is accessed using Outlook Web Access from any Internet connected computer.

Text Messaging (SMS/MMS) – Text messaging or multimedia messaging refers to brief written messages exchanged between portable devices, typically over a wireless network. These messages may also contain photos, videos, or audio files. Pagers are devices that can receive text messages, but typically cannot transmit or respond to messages. "Chatting" or instant messaging between computers is also considered text messaging.

PROCEDURE

Computer Use

Only Sheriff's Office owned and/or leased computers shall be used by employees while on duty and only for purposes related to achieving the Sheriff's Office mission. For any and all County owned computers or computer systems, there shall be no expectation of privacy. All County owned computers or computer systems, as defined in this order, are subject to periodic and unannounced audits to ensure compliance with this order. Personally owned computers such as laptops, hand held devices and other similar computer devices may be used only with prior written approval from the employee's Division Commander, and cleared through TSU. No personally owned computers or computer systems shall be connected to the MCSO network at any time, without proper prior approval from the employee's Division Commander, and cleared through TSU. Such a connection includes, but is not limited to, VPN (virtual private network) or direct connection via LAN port (local area network).

Only authorized, Sheriff's Office owned, licensed software will be installed and used on any Sheriff's Office computer. No employee will install or use any personally owned or unlicensed software on any Sheriff's Office computer system. Any employee or division wishing to acquire and use any software that varies from the Sheriff's Office standard must receive prior written authorization from the Division Commander.

No changes or modifications to any computer or computer system configuration will be made by any employee except authorized Sheriff's Office Technology Services Unit staff. No attempt will be made by any employee to bypass or circumvent any computer or software security in order to make any modifications, or add or remove any software. The exception to this section includes employees who exclusively use a "single-user" computer. These employees may make minor modifications to the general appearance and functionality of their computer to accommodate personal working style.

Those employees using a "single-user" computer may password protect their computer at initial startup. All computer passwords will be submitted to the Administration and Support Services Captain, or his/her designee, who will maintain a list of all passwords in case access to the computer is needed. This does not apply to Windows logon passwords or other application passwords, which should not be submitted to the Administration and Support Services Captain.

No hardware additions, deletions or modifications will be made to any Sheriff's Office computer system by any employee with the exception of Sheriff's Office Technology Services Unit staff authorized by the Administration and Support Services Captain. This includes repairs to Sheriff's Office computers unless directed by Sheriff's Office Technology Services Unit staff. This does not preclude the Administration and Support Services Captain from assigning a division manager the responsibility of maintaining his/her division's computers or computer systems.

Any use of computers or computer systems, while driving or operating a motor vehicle, must be operated in a hands free manner.

Email

All Sheriff's Office employees will have an email account. Email shall only be used for purposes related to achieving the Sheriff's Office mission. Email shall not be used for personal messages or private business. The exception would be short and infrequent messages to arrange or confirm appointments, or inform family of overtime work, etc.

There shall be no expectation of privacy in either type of email message, either sent or received, all of which are subject to periodic and unannounced audits to ensure compliance with this order.

The transmittal, intentional retrieval, or storage of any digital files that are racist, sexist, threatening, discriminatory, harassing, obscene, pornographic, or X-rated is strictly prohibited unless specifically

related to the employee's immediate law enforcement task and only with the express written permission of the employee's Division Commander. Any employee who receives any information of this nature must immediately notify his/her supervisor in writing. Failure to do so will result in a presumption that the employee intentionally downloaded and/or retained the material in question.

Employees must remember that email is not secure and they must consider that fact when transmitting information of a highly sensitive or confidential nature.

Employees must be aware that email attachments can contain computer viruses. Employees must take appropriate precautions when downloading or opening email attachments. Oftentimes, the best course of action is to delete the suspect email or attachment without opening it. Employees shall immediately report, in writing, all incidents of suspected computer viruses to Sheriff's Office Technology Services Unit.

All Sheriff's Office employees have remote access to their email accounts from computers or other devices outside of the Sheriff's Office network using Outlook Web Access. This is typically used by employees to access email, calendar, and contacts from their personal computers or other devices at home. This remote email service is provided to employees as a convenience, and there is no expectation that employees will monitor their email accounts while off duty. Work performed remotely during off duty hours is not authorized unless performing that work has been previously approved by the employee's supervisor, consistent with all other applicable rules, regulations and general orders.

While the mechanism to access email accounts remotely is secure, caution must still be taken when accessing email from computers or other devices outside the Sheriff's Office network. Employees shall only access their email accounts from trusted computers, such as their personal computer at home. Because of the ease with which user names and passwords can be captured without an employee being aware, email shall not be accessed from untrusted computers or other devices, such as public use computers, Internet cafés, or Internet kiosks in public areas. Care should also be taken when viewing content of a sensitive nature that could potentially be viewed by others. Any personally owned computer or computer system that has been set up to automatically receive Sheriff's Office email (such as cellular phones / tablets etc), that is lost or stolen, must be reported to TSU immediately. TSU will then attempt to remotely wipe the device to ensure proper security is maintained.

Internet

All Sheriff's Office computers connected to the local area network have Internet access. With the exception of limited personal use as outlined below, department employees shall access the Internet while on duty only for purposes directly related to work being performed by that employee in furtherance of the Sheriff's Office mission.

There shall be no expectation of privacy in any Internet or World Wide Web access, either of which is subject to periodic and unannounced audits to ensure compliance with this order.

Accessing, viewing, posting or sharing of any material that is racist, sexist, threatening, discriminatory, harassing, obscene, pornographic, or X-rated is strictly prohibited unless specifically related to the employee's immediate law enforcement task and only with the express written permission of the employee's Division Commander. Any employee who receives any information of this nature or inadvertently views a web site or page containing material of this nature must immediately notify his/her supervisor in writing. Failure to do so will result in a presumption that the employee intentionally received, retained, or visited a site or page containing the material in question.

Employees, other than those currently assigned to the Sheriff's Office Technology Services Unit, shall not download or install any software programs from the Internet without the permission of the Administration and Support Services Captain.

Limited Personal Use

Reasonable and limited personal use of county owned computer systems and internet is permitted. Use of Sheriff's Office or County owned computers, applications, or internet for personal use shall be kept to a minimum. Such use will be brief and conducted during approved breaks, or as otherwise specifically authorized by the Sheriff or his designee. During limited personal use, employees shall not view or access any prohibited material or electronic media as defined in the 'Internet' section of this policy.

Activity and Content Monitoring

No employee shall have any expectation of privacy or confidentiality when using any Sheriff's Office owned or operated device, system, or application described in this order. Activity and content is routinely monitored and logged, and may be reviewed or audited at any time, with or without notice to the employee.

RELATED STANDARDS:

Marin County Personnel Management Regulation 23

AFFECTED DIVISIONS:

All

DATE OF REVISIONS:

07/16/10
11/23/09
11/5/09
6/12/08
5/10/00
05/03/16
10/18/16

By order of:

ROBERT T. DOYLE
SHERIFF