A
17-032
2/2/17

SFPD Members' Expectation of Privacy
Use of Computers, Peripheral Equipment and Facilities

(Re-issue DB 13-165, Amends portions of DGO 10.08)

This bulletin updates Department General Order 10.08, Use of Computers and Peripheral Equipment.

Use of Computers and Peripheral Equipment

1. Official Use Only. The Department provides members' access to City computers, City-issued electronic devices, including Department issued Smart Phones, MDT/ MVT, databases, systems, and software, as well as the City's internet link and electronic mail (email) system, to use for authorized, official City business only. Members may not use, or allow any other person to use, City computers, phones, the internet link or email system for any non-City purpose, including but not limited to personal, political, or employee associations or organizations' business.

Inappropriate uses of Department electronic resources include, but are not limited to: viewing or distributing materials that are sexually explicit; viewing or distributing materials that violate DGO 2.09, 10.08, or 11.07; viewing sports or other events online; playing games or streaming video or music on a work computer; maintaining or participating in non-work related web logs ("blogs"), web journals, and chat rooms; soliciting funds; running a personal business; engaging in political activity; and creating or distributing chain emails or unsolicited commercial emails ("spam").

Sworn members whose specific investigative duties are related to human trafficking or adult or child exploitation may access pornographic sites or internet sites associated to their duties when:

1. A commanding officer gives written permission to the officer; and
2. The work is performed on a SFPD device; and
3. The account is either an official SFPD account or account is authorized by a commanding officer; and
4. Open access is allowed by the Technology Division; and
5. Access shall be conducted during on duty hours and at the work site.

2. NO EXPECTATION OF PRIVACY. Members are reminded that their use of City computers, City-issued electronic devices and the City's internet link and email system is not private and have no expectation of privacy. The Department randomly audits all official electronic communications, Department issued email accounts, communications on mobile terminals and text messages on Department issued phones. The Department randomly monitors, accesses, retrieves or deletes any information, record or site that a member viewed, created, stored, received or sent over the Department's computers, internet link and email system, for any reason, with or without cause or notice, at any time and without a member's permission. This includes monitoring and reviewing emails, personal or private instant messages, and use of the internet and intranet, including time spent on the internet and websites visited. Because City computers may be accessed by other authorized users, members should not store on a work computer, or phone, any information the member does not intend to share with others.

If a member uses a Department computer, City-issued electronic device, internet link or email system to send or receive non-City records or information that are subject to any confidentiality or privilege, including but not limited to the attorney-client privilege, the member waives whatever rights he or she may have to assert such confidentiality or privilege against disclosure.

3. Confidentiality of Data and Systems. All members must protect the integrity of the Department's confidential information, as well as the confidential information in databases and systems to which the Department has access, including but not limited to the California Law Enforcement Telecommunications System ("CLETS"). Members shall not access Department data except as needed to perform their work duties. Members shall not access computers, networks, servers, drives, folders or files to which he or she has not been granted access or authorization from an authority who can grant access. Members shall not defeat, attempt to defeat, or compromise security restrictions on Department computers, City-issued electronic devices, systems and applications.

Members accessing CLETS are subject to CLETS policies and procedures. Members shall not send criminal history information by email or the internet.

Members shall not destroy, delete, erase, conceal, release or disseminate Department information, records or other data without authorization, and shall not otherwise make that information, files or data unavailable or inaccessible to the Department or other authorized users of the Department's systems.

Members shall promptly report any lost or stolen electronics and/or devices to their supervisor.

For the Department to meet public record and record retention requirements, members shall use only their Department email for conducting Department business.

4. User Names and Passwords. User names and passwords exist to protect City information, records and systems. Members shall use their own Department-issued user name and password to log onto City computers, systems, City-issued electronic devices and shall not use any other user name or password. Members shall be responsible for all computer access logged under their user name and password.

Members shall not disclose their user names or passwords to any other person, with the following exceptions:

A. to an authorized member of the Technology Division;

B. upon a proper order by a member conducting an administrative investigation; or

C. pursuant to an order from the Chief of Police.

Members shall log off any computer, City-issued electronic device or system if the member leaves the computer or electronic device unattended.

5. Representing the City and Department. When communicating by the internet or email, members shall remember that they represent the City and the Police Department. Members should be aware that posting on the internet and participating in web-based communications may identify them as a Department member. Members shall review their communications to ensure they

accurately convey the Department's position and provide information in a professional, courteous and respectful manner. Members shall not impersonate another when communicating by the internet or email without prior written approval from their Commanding Officer as part of an official investigation.

6. Viruses. Members shall follow all procedures that may from time to time be issued by the Technology Division to protect the Department's systems from viruses. Members shall not deliberately propagate any virus, worm, Trojan horse, trap-door program code or other code or file to disrupt, disable, impair or otherwise harm either the Department's networks or systems or those of any other individual or entity.

7. Software. The Department has purchased or licensed the use of certain commercial software programs, databases and systems for business purposes. Members may use these only for official work purposes. Members may not duplicate or alter these licensed software programs or databases. In addition, members may not install or use unauthorized software programs on City computers, City-issued electronic devices or systems.

8. Personal Devices. Members shall not connect a personal computing device, data storage device, image-recording device or auxiliary electronic device to any Department computer or other electronic resource, except in the performance of their official duties.

9. Copyright and Trademarks. The ability to easily retrieve information and records from the internet and transmit those by email increases the risk that a member may infringe third-party intellectual property rights. Members shall observe and abide by all copyright, trademarks, service mark restrictions and other intellectual property rights in distributing or posting materials. Members shall not copy from or distribute via the internet or email any material (such as software, database files, documentation, articles, graphics files or other data) if the author has posted restrictions on the use or reproduction of the material. Members who are unsure whether it is permissible to access, copy or distribute material shall contact the Legal Division.

Use of Facilities

No Expectation of Privacy. Members are reminded that there is no expectation of privacy during any communication or conversation while using common areas of any Department location or facility, at Department sponsored trainings or events, or at any activities where a member represents the Department.

William Scott
WILLIAM SCOTT
Chief of Police

Per DB 15-141, both sworn and non-sworn members are required to electronically acknowledge this Department Bulletin in HRMS.

Complies with DOJ recommendation #24.4.