USE OF ~~COMPUTERS AND PERIPHERAL EQUIPMENT~~ELECTRONIC RESOURCES

This order establishes policies and procedures governing the use of ~~computers and the~~ electronic resources, confidentiality and expectation of ~~computer~~privacy.

Definitions

Electronic Resources - includes all digital data driven devices, including but not limited to desktop PC, portable devices such as laptops, security tokens, Mobile Data Terminal (MDT), tablets and mobile data device, networks including wireless, internet & intranet connectivity, email, external storage devices, databases, law enforcement applications, business applications, peripherals like printers, scanners, blue tooth devices, USB, portable external drives, accessories, software and firmware associated there within.

Electronic Devices - will be used to define the hardware provisioned to access official duties and is considered as a subset of Electronic Resources.

Members – refers to all SFPD employees, sworn and civilian.

10.08.01
POLICY

The policy of the ~~D~~department is to protect all confidential information from unauthorized access, disclosure and ~~access and~~ require responsible use of ~~all computers,~~ electronic ~~mail and~~resources. It also outlines members' expectations to privacy in either written or oral communications in any form while in the ~~Internet~~employment of, or representing the San Francisco Police Department.

10.08.02
PROCEDURES

~~A. USERNAMES AND PASSWORDS~~

A. AUTHORIZED USE OF ELECTRONIC RESOURCES

Electronic Resources are provisioned

1. ~~All~~ access to ~~computer use and the data contained within is protected by the use of individual user names and passwords issued to a member by the~~

Department. No member shall access any Department computercity employees for any purpose by using a user name and password other than those issued to the member by the Department.

2. authorized official city business use only. Members shall maintain the confidentiality of their Department-issued user name and password. Members shall may not disclose their username and password touse, or allow any other person with the following exceptions:

A. Authorized members of the M.I.S. Unit;

B. Upon the request of an officer conducting an administrative investigation;

1. Pursuant to an order from the Chief of Police.

3. Members shall be responsible for **all** computer access as logged under their user name and password.

to use, department provisioned electronic resources

4. If a member forgets his or her user name and/or password, the member shall request a new user name and/or password by submitting a memorandum through the chain of command to the Deputy Chief of Administration. When the Deputy Chief of Administration approved the request, the MIS Unit will issue a new user name and/or password to the member.

B. ISSUANCE OF DEPARTMENT EQUIPMENT

1. The Deputy Chief of Administration through the MIS Unit shall authorize the distribution of all computers owned or controlled by the Department. This includes computers obtained through purchase, donation, seizure, forfeiture, unclaimed property and grants.

2. A member requesting any computer equipment (hardware or software) shall forward a memorandum through the chain of command to the Deputy Chief of Administration. The memo shall include the member's reason for requesting the equipment and any known or potential funding source.

3. No member shall modify any Department computer equipment or install any device or program, including but not limited to any peripherals such as external storage devices, printers, scanners or any type of communication device without written approval of the Deputy Chief of Administration.

C. USE OF PERSAONLLY OWNED COMPUTERS

~~1. A member who requests permission to use owned computer for Department purposes shall submit a memorandum through the chain of command to the Deputy Chief of Administration. The memo shall include the make(s), model number(s) and serial number(s) of all hardware components and the manufacturer(s) title(s), version number(s) of all software loaded on or that may be loaded on the computer.~~

personal, political, or employee associations or organizations' business. No member shall

~~2. Members shall not use software obtained in violation of copyright laws.~~

~~3. The Department shall not be responsible for the repair, maintenance or upgrade to personally owned computer hardware or software. Any damage to personal property shall be governed by DGO 3.15.~~

~~D. UNAUTHORIZED USE OF OFFICE TECHNOLOGIES~~

~~Members may use Department owned and issued equipment, including computer equipment, for work related purposes only.~~

1. ~~No member shall~~ use access to e-mail, the ~~Internet~~internet, or any computer program for any purpose other than those reasonably necessary for the performance of his or her work assignment. (Penal Code **§** *502).* ~~Members are specifically prohibited from using e-mail or Internet accounts to access~~

2. Inappropriate uses of department electronic resources include, but are not limited to, viewing or distributing materials that are sexually explicit; 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; or creating or distributing chain emails or unsolicited commercial emails ("spam").

3. Sworn members whose specific investigative duties are related to human trafficking or~~,~~ adult or child exploitation may access pornographic sites or other social media and internet sites associated to their duties when the work is approved through chain of command and is performed during on duty hours at SFPD premises using department electronic devices approved by the Technology Division.

~~2.~~4. All members are specifically prohibited from using e-mail, texting, social media or internet accounts to access information reasonably considered offensive or disruptive to any member. Offensive content includes, but is not limited to, sexual comments or images, racial slurs, gender-specific comments, or any comments, that would reasonably offend someone on the basis of age, sexual orientation, religious or political beliefs, national origins or disability.

5. Emails, texts, documents and all other content on department electronic resources are not private. For the department to meet public record and record retention requirements, members shall use only their department email for conducting department business.

B. CONFIDENTIALITY OF DATA AND SYSTEMS

1. All members must protect the integrity of the department's confidential information and must acknowledge the acceptable use policy each time they login to an SFPD workstation.

2. All members must protect 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").

3. Members shall not access department data except as needed to perform their work duties.

4. 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.

5. Members shall not defeat or attempt to defeat security restrictions on department computers, department electronic devices, systems and applications.

6. Members accessing CLETS are subject to CLETS policies and procedures.

7. Members shall not send criminal history information by email or the internet.

8. 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.

C. EXPECTATION TO PRIVACY

Members are reminded that their use of department-issued electronic resources is not private. The Technology Division may monitor, access, retrieve or delete any information, record or site that a member viewed, created, stored, received or sent over the department's network, internet link and email system for any reason, with or without cause or notice, at any time and without a member's permission. This may include 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. Department provisioned electronic resources may be accessed by other

authorized users, members should not store any personal information which the members does not intend to share with others.

If a member uses a department-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 the member ~~he or she~~ may have to assert such confidentiality or privilege against disclosures.

~~Use of City Facilities.~~ 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

D. PUBLIC RECORDS ON PERSONAL ELECTRONIC DEVICES

The California Supreme Court has ruled (*City of San Jose v.* Superior Court ("San Jose"), --- Cal.4th ---, 214 Cal.Rptr.3d 274, decided March 2, 2017) that communications on personal electronic devices ("PEDS") of City employees and officials may be public records subject to disclosure under the California Public Records Act ("CPRA"). Accordingly, members may not avoid public records laws by doing the public's business in private—records of public business on PEDs must be as accessible to the public as electronic records on the City's own devices.

Guiding principles that members should keep in mind:

1. Communications on PEDs or personal accounts involving the conduct of the public's business may be public records subject to disclosure. Such writings include, but are not limited to, emails on personal computers and text messages and voice messages on personal cell phones. They include not only messages written by members on PEDs, but also messages received.

2. Not all communications on PEDs are public records. Only a "writing containing information relating to the conduct of the public's business"—that is, a writing that itself serves, or is intended to serve, a City purpose and that involves a matter over which the member has work responsibility—is a public record. "Work responsibility" here is a broad concept. It goes beyond work required of the member and includes work voluntarily assumed. The basic test is whether the writing on the PED serves or was intended to serve at least - in part - a police function. If the writing serves an essentially private function, it is not a public record. If it contains primarily personal information, with only incidental references to City business or department related business, it is very likely not a public record. Beyond these general principles, a number of factors, including content, context, and intended recipients, determine whether the writing is a public record. When both the sender and recipient of the

writing are members, and the writing involves police business, there is a good chance it is a public record.

3. Members are responsible for searching and retrieving responsive records on their PEDs in response to a public records request. Members are responsible for determining whether a writing is a public record using the test described in point 2, above. A public record is:

   a. Any writing, regardless of physical form or characteristics;
   b. Containing information relating to the conduct of the public's business; and
   c. Prepared, owned, used, or retained by a state or local agency. Cal. Govt. Code § 6252(e).

The definition of a "writing" is extremely broad and encompasses any handwriting, typewriting, printing, photostating, photographing, photocopying, transmission by e-mail or fax, and every other means of recording on any tangible thing any form of communication or representation, including letters, words, pictures, sounds, or symbols. Cal. Govt. Code § 6252(g). The writing is considered that of the agency—the department—if it meets the test described in point 2, above. In a court proceeding concerning the request, members must be prepared to testify under oath or submit a statement under penalty of perjury, describing the search conducted on the PED and explaining the types of writings on the PED that were not provided to the requester because they were non-responsive.

4. The CPRA exempts from disclosure certain types of records. For example personnel or similar records, the disclosure of which would constitute an invasion of privacy and records of ongoing police investigations are exempt. There are many other exemptions that are found in DGO 3.16. The *San Jose* decision does not change the exemptions from disclosure for public records or the rules governing withholding or redaction of public records. A public record on a member's PED is no different from the identical record on a computer or other electronic device belonging to the department. The possible exemptions are the same, and they apply equally to public records on PEDs.

5. The *San Jose* decision does not change records retention requirements. A public record on a member's PED is no different from the identical record on an electronic device belonging to the department. Records retention and destruction policies apply equally to public records on PEDs. But there is no requirement that members keep the records on PEDs, even if they must be retained, so long as they appropriately transfer those records onto department devices where they will be retained.

6. A public records request need not specify that it seeks records on members' PEDs for such records to be covered by the request. Members shall search their PEDs for responsive records unless otherwise directed by Legal Division.

7. In searching and retrieving responsive records from their PEDs, members may need assistance in determining whether a particular record on a PED, is: (1) a public record, (2) exempt from disclosure or (3) subject to retention. They may contact the Legal Division at (415) 837-7394 for assistance.

All members shall use department issued electronic devices for official business except in emergency situations. In an emergency, members may use their own personal electronic devices for official department business. For example, an emergency arises when a member's department issued device is damaged or unusable, and the member must call or text his or her commanding officer for official department business.

E. REPRESENTING THE CITY AND THE DEPARTMENT

When communicating by the telephone, 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.

1. No member shall ~~Only the MIS Unit may create, administer and maintain e-mail or Internet account on Department owned or issued computers, and may do so only with the approval of the Deputy Chief of Administration. Any member requesting an e-mail or Internet account shall do so by submitting a memorandum through the chain of command to the Deputy Chief of Administration.~~

2. ~~No member shall access any criminal history information except as necessary for a bona fide criminal investigation. No member shall access computer history information for curiosity, personal or political purposes. All members accessing confidential criminal history information shall be familiar with Department rules and regulations and local, state and federal laws regarding proper access and use of such information.~~

~~E. PRIVACY OF COMPTER INFORMATION~~
convey official department

1. ~~Members shall not~~ ~~have an expectation of privacy for information stored or accessed through Department owned or issued computer equipment. Authorized Department personnel may access information stored or contained on any Department computer, and may log and monitor network activity, without notice at any time. This includes monitoring and logging Internet and e-mail use. Members shall not create any unauthorized security barriers to the Department's access to their computer or files.~~

~~F. DISSEMINATION OF INFORMATION THROUGH THE INTERNET~~

~~1. THE DEPARTMENT'S OFFICIAL WEBSITE. The City's Department of Telecommunications and Information Services (DTIS) administers the Department's official Web Site. Any member requesting the addition of any information to the Department's Web Site shall submit the request by memorandum through the chain of command to the Deputy Chief of Administration. If approved by the Deputy Chief of Administration, the MIS Unit will submit the request to DTIS.~~

~~HOME PAGES AND OTHER INTERNET SERVICES. No member shall convey official Department~~ information, or make any representation, actual or implied, that he or she is conveying official ~~Department~~department information on any website or in any other form through the ~~Internet~~internet, other than through the ~~Official Department Website, except with~~official department website. Any content that is published on department website(s) are to be approved by the ~~express written permission~~chain of command for their respective content areas. Members who are authorized to use social media to post and respond to public channels are performing official SFPD work and technology team may assist in publishing the ~~Deputy Chief of Administration~~content, provided appropriate approvals are in place.

F. PERSONAL ELECTRONIC DEVICES

Members shall not connect a computing device, external 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. The department shall not be responsible for the repair, maintenance or upgrade to personally owned computer hardware or software. Members shall not use software obtained in violation of copyright laws. Any damage to personal property shall be governed by DGO 3.15.

G. 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 department computers, department-issued electronic devices or systems.

H. 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.

I. COPYRIGHTS AND TRADEMARK

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.

J. ISSUANCE OF DEPARTMENT ELECTRONIC RESOURCES

The Director of Technology Division shall authorize the distribution of all electronic devices owned or controlled by the department. This includes computers, mobile devices and/or other electronic devices, software(s) obtained through purchase, donation, seizure, forfeiture, unclaimed property and grants. If an 'electronic resource' is not already provisioned to the member of the department, it can be requested through a formal approved memorandum through the member's chain of command to the member's deputy chief. The memorandum shall include the member's reason for requesting the equipment and any known potential funding source.

K. USERNAMES, PASSWORDS & TOKENS

User names, passwords and tokens exist to protect city information, records and systems. Members shall use their own department-issued user name, password and token to log into department computers, mobile data devices and other department issued electronic devices. Members shall be responsible for all computer access logged under their user name and password. Members shall not disclose or share their user names, passwords or tokens with any other person, with the following exceptions:

1. Upon a proper order by a member conducting an administrative investigation; or
2. Pursuant to an order from the Chief of Police.

~~G. RESPONSIBLIIES OF THE MANAGEMENT INFORMATION SERVICES (MIS) UNIT~~

Members

~~The~~ ~~MIS Unit~~ shall log off any electronic device before leaving the electronic device unattended.

If a member forgets ~~his~~~~be~~ ~~/her~~ a network username and/or password, the member shall contact the Technology Division by emailing SFPDHelpDesk@sfgov.org or by calling the SFPD Help Desk at (415) 558-3877 for resolution.

L. E-MAIL

1. The department assigns each member an individual email account for official department business only. Members are responsible for~~:~~ monitoring their department email accounts at least once during the course of each shift. Members shall read and respond to (as necessary) any new messages in the Inbox. Members will be held accountable for information and documents transmitted by email.

2. Members shall provide their department email address to the public when asked or when email correspondence might aid in an investigation or otherwise assist with follow up.

3. Members shall create a signature within their email that includes their name, rank, star number, assignment and unit phone number.

4. Members shall use the "out of office" notification when a member expects to be away from work for more than three (3) working days.

5. Email is intended and designed to be a tool of transmission and not a tool for storage of information. Email systems are not meant for storage or maintenance of permanent records. Members should refer to the city attorney's 'Good Government Guide' for questions about the retention of email in accordance with the department's record retention and destruction schedule and policy. Alternately, members should direct any questions to SFPD Legal Division at (415) 837-7394.

6. Members shall not use their personal email address for official city business. Under the Sunshine Ordinance and the California Public Records Act, an email created or received using the city email system is a public record and may be subject to disclosure unless a specific exemption applies.

7. The "SFPD Everyone" group email address and the "Reply All" response is intended for critical or essential information that requires immediate dissemination to all members. With the exception of otherwise approved sources, i.e. Written Directives, Technology Division, Academy Training,

Station Investigation Teams (SIT) and Investigation Bureaus, members shall obtain prior approval from their Officer-in-Charge (OIC) of any email communication they send to "SFPD Everyone.". Members shall ensure the approving OIC receives a courtesy copy of the email prior to sending it to "SFPD Everyone.".

8. Email messages received should not be altered without the sender's permission; nor should email be altered and forwarded to another user and/or unauthorized attachments be placed on another's email message.

M. USE OF MOBILE DATA DEVICE

1. Members shall be responsible for the protection and proper use of the department-issued mobile data device, which includes token, and any data accessed with it. Members shall carry the devices while on-duty and ensure they are operational and in good functioning order at the start of their tour of duty.

2. Members shall use the protective case provided with their department-issued mobile data device at all times.

3. Members shall not add, alter, install, delete, upgrade, replace, reconfigure or otherwise modify department-issued mobile data device software, except as authorized through the Technology Division. This includes, but is not limited to, the operating system, applications and security settings.

4. Members shall not enter into their own service or support contracts, licensing or purchasing accords, or any other third-party agreements regarding a department- issued mobile data device.

5. Members shall connect the department-issued mobile data device to only known secure Wi-Fi networks.

6. Members who as a part of their duties are required to be instantly available to return to work to perform their duties when they are normally off-duty (for example, an 'on-call' investigator) shall keep their department-issued mobile data device powered on and readily available for the duration of such obligation.

7. Off-duty members are not required to keep their mobile data device powered on when not working and are not entitled to compensation for use of the department-issued mobile data device.

8. Members should refrain from using a department-issued mobile data device while driving unless there are articulable exigent circumstances. (Ref; 23123 CVC, 23123.5 CVC)

N. REPLACEMENT

1. If a department-issued mobile data device is discovered lost or stolen, the member shall immediately notify the SFPD Help Desk at (415) 558-3877 so that data on the device may be remotely deleted and the device disabled.

2. Members shall ensure they receive a claim number from the SFPD Help Desk regarding the incident. Members shall include the claim number in the memorandum and incident report and submit both through their chain of command regarding the loss, theft, or damage of any department-issued electronic resource.

3. Members shall hand carry a malfunctioning device to the Technology Division for service or replacement as soon as feasible.

10.08.03 RESPONSIBILITIES OF TECHNOLOGY DIVISION

The Technology Division shall be responsible for:

1. Acquiring, installing, repairing, maintaining and replacing all ~~Department owned or issued computer hardware and software, including peripherals~~department owned electronic resources.

2. Arranging and managing all ~~computer~~ support/maintenance agreements with vendors.

3. Registering all ~~computer hardware and software and shall be the~~ electronic resources as Registered Licensee.

4. Inspecting and auditing all ~~Department computer equipment~~department-issued electronic devices including software.

5. De-commissioning of electronic resources as necessary.
6. End-User Support of department-issued electronic resources for members.
7. Support is provided during weekdays Mon-Fri from 8am PST to 5pm PST through SFPD Help Desk Phone Number (415) 558-3877, email SFPDHelpDesk@sfgov.org or walk-in to Technology Division at Police Headquarters (4th Floor, 1245 Third Street, San Francisco, CA, 94158)
8. For production system down issues, Department of Emergency Management (DEM) engages on-call support engineers to provide off-hours and weekend support. Users should call (415) 558-3877 to report the issue and expect a response back from SFPD Technology member within 4 hours.

References

DGO 2.01, General Rules of Conduct
DGO 3.15, Personal Property Claims
DGO 3.16, Release of Police Reports
DGO 10.06, Uniform and Equipment Issuance and replacement
DGO 10.07, Use of Cellular Telephones
DGO 10.09, Computer Management Committee
DGO 11.07, Prohibiting Discrimination, Harassment and Retaliation
City Attorney's 'Good Government Guide'