DEPARTMENT NOTICE

21-168
11/19/21

Public Records on Personal Electronic Devices

(Supersedes DN 21-120)

The City Attorney's *Good Government Guide*, has long advised that "while courts have not definitively resolved the issue, City officials and employees, in an abundance of caution, should assume that work they perform for the City on personal computers or other personal communications devices may be subject to disclosure under the public records laws." (*Good Government Guide,* 85.)

The California Supreme Court has now definitively resolved this issue. In *City of San Jose v. Superior Court ("San Jose")*, --- Cal.4th ---, 214 Cal.Rptr.3d 274, decided March 2, 2017, the Court ruled 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.

Here are some guidance 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 1) any writing, regardless of physical form or characteristics; 2) containing information relating to the conduct of the public's business; and 3) prepared, owned, used, or retained by a state or local agency. Cal. Govt. Code § 6252(e). The definition of a "writing" is extremely broad. It encompasses any handwriting, typewriting, printing, photostating, photographing, photocopying, transmission by email 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 the disclosure of 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. Many other exemptions 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 their commanding officer for official department business.

Other exceptions would include telecommuting or when using your approved remote desktop to access the Department Active Directory or other approved applications such as for RSA Authenticate, SFPD email, and AnyConnect for official police business. Any transfer of law enforcement information or data outside SFPD applications to your personal electronic device or personal applications may be subject to disclosure under the current California Public Records Act.

Members using personal electronic devices for telecommuting must have successfully completed the Telecommuting Training Course and received prior approval from your supervisor.

Reference:
DGO 10.08 Use of Computers and Peripheral Equipment

William Scott
WILLIAM SCOTT
Chief of Police

Per DN 20-150, sworn & non-sworn members shall electronically acknowledge this Department document in PowerDMS. Members whose duties are relevant to this document shall be held responsible for compliance. Any questions regarding this policy should be made to sfpd.writtendirectivessfgov.org who will provide additional information.