

**Office of  
The City Attorney  
City of San Diego**

**MEMORANDUM  
MS 59**

**(619) 533-5800**

**DATE:** October 9, 2019

**TO:** Kris Michell, Chief Operating Officer  
Ron Villa, Assistant Chief Operating Officer  
Jonathan Behnke, Chief Information Officer

**FROM:** City Attorney

**SUBJECT:** Online Collaboration Tools

---

**INTRODUCTION**

City of San Diego departments have increasingly embraced new technologies to improve communication, teamwork, and service levels. Especially popular are online collaboration tools such as *slack*, *asana*, *Google G Suite*, and *Yammer*.<sup>1</sup> While these technologies are useful and innovative, care must be taken to ensure the City meets the legal responsibilities for transparency required of local governments by retaining and producing records in accordance with the law, including the City's record retention policies and the California Public Records Act (CPRA). This memorandum provides legal guidance to City departments and employees considering using online tools as part of their business process.

**DISCUSSION**

**I. Contracting Issues**

Online collaboration tools often require a customer to agree to Terms of Service regarding the use of their product. The Terms of Service may constitute a binding contract with the user, and potentially with the organization that the user purports to represent. The terms of this contract could affect the City's legal liabilities and the City's access to its own data.

Before agreeing to Terms of Service, an employee should ensure that the terms comply with City contracting regulations<sup>2</sup> and that he or she has the necessary authority to enter into a contract on behalf of the City. In fact, *slack* advises users to "make sure you have the necessary authority to

---

<sup>1</sup> As an example, the *slack* platform provides instant messaging, document storage, to-do lists, and calendaring functions. It is hosted on remote servers owned by a private company, with users providing their own personal login information and optionally setting their own data retention periods.

<sup>2</sup> City contracts must comply with competitive bidding requirements depending on the dollar value of the contract and include certain mandatory contracting provisions. City Att'y MOL No. 2015-12 (July 14, 2015).

Kris Michell, Chief Operating Officer  
Ron Villa, Assistant Chief Operating Officer  
Jonathan Behnke, Chief Information Officer  
October 9, 2019  
Page 2

enter into the Contract on behalf of [your organization] before proceeding.” *Slack* (April 4, 2019), <https://slack.com/terms-of-service/user>.

Only the Mayor and the Mayor’s specifically authorized designees have the power to execute contracts for departments under the Mayor’s control. San Diego Charter § 28, Memorandum from Mayor Kevin L. Faulconer, City of San Diego, on Delegation of Authority to Sign Contracts, to Department Directors (September 24, 2018) (On file with the Office of the City Clerk). In addition, City contracts should be signed as to form by the City Attorney’s Office. San Diego Charter § 40.

For these reasons, and electronic data retention issues discussed in Section II.C below, it may be advisable for the City to enter into a master contract with the vendor under which employees may open individual accounts.

## **II. Retaining Electronic Communications**

Online collaboration tools must be used in a manner that complies with the City’s records retention rules.

### **A. Records or Nonrecords**

The content generated using online collaboration tools may constitute “records” subject to mandatory retention periods. The San Diego Municipal Code (SDMC) requires retention of City records according to the Master Records Schedule, or until the termination of a legal hold.<sup>3</sup> SDMC § 22.2606 (incorporating retention periods defined by local, state, and federal law). The SDMC also provides a definition for what constitutes a City record:

Record means recorded information of any kind and in any form, created or received by the City that is evidence of its operations. Records include paper and electronic documents, electronic databases, electronic mail, correspondence, forms, photographs, film, sound recordings, maps, and other documents that have administrative, legal, operational, fiscal, or historical value requiring retention of the record for a specified period of time.

SDMC § 22.2602 (Italics omitted).

The City Administrative Regulations also make it clear that such City records may include content hosted by online collaborative platforms: “Social media and tools that facilitate

---

<sup>3</sup> Legal hold means a communication issued by the City as a result of current or anticipated litigation, a notice of audit, or a government investigation. SDMC § 22.2602.

conversation, including, but not limited to, Instant Messaging, Twitter, Facebook, YouTube, LinkedIn, and blogs, may be a record subject to retention.” San Diego Admin. Reg. 85.10 § 2.10.

The Municipal Code provides further guidance by defining what is *not* a record. A nonrecord is recorded information of any kind “which is not required to be retained in the ordinary course of City business or is a temporary aid and does not appear in the Master Records Schedule.” SDMC § 22.2602 (*italics omitted*). In the context of online collaboration tools, nonrecords might include any messages that are not created for the purpose of preserving documentary or informational content for future use by the City (*id.*) (e.g., rough notes or brainstorming, personal invitations, or a question to a colleague).

To illustrate these principles, we have included a chart analyzing *slack* advertising claims to determine whether content is likely to contain City records. *Slack* advertises that “[i]t’s a place where conversations happen, decisions are made, and information is always at your fingertips.” *Slack* (April 4, 2019), <https://slack.com>:

<b>Activity:</b>	<b>Summary Analysis:</b>	<b>Basis:</b>
<i>conversations happen</i>	May be a City record.	Messages that are created or received in connection with official City business; messages that initiate, authorize, or complete a City transaction.
<i>decisions are made</i>	City record.	Messages that document the formulation or execution of City policies and decisions.
<i>information always at your fingertips</i>	Likely a City record.	Documents made or retained for the purpose of preserving its informational content for future reference.

In sum, when decisions, policies, procedures, or standards are announced using an online tool, a court is likely to find that the intended purpose is to document the content for future reference by a department’s employees; this purpose gives rise to “record.” This is true regardless of the format of the message or the application’s retention period setting. Therefore, City departments and employees have a duty to ensure proper retention of content generated using online collaboration tools.

## **B. Master Records Schedule**

The City is currently transitioning to a Master Records Schedule (MRS) with a single record retention schedule for all City records. Until the transition to the MRS is complete, departments should follow the requirements of the General Records Disposition Schedule (GRDS) and department specific Record Disposition Schedules (RDS). If a document or electronic content

appears on the GRDS or the applicable RDS, it must be retained. Once an electronic communication is determined to be a City record, it must be retained according to the retention periods set forth in the RDS. SDMC § 22.2606.

The GRDS provides guidance for electronic mail that is also helpful when evaluating instant messages, electronic communications, or any content hosted on an online collaboration platform. Note that the GRDS distinguishes the format of the record from the content, and requires removing a City record from the electronic system, then printing and storing it with the file of related content, or maintaining it in a “secured system” that may be accessed and searched by a department’s records coordinator. This is extremely important in the event that a City employee in possession of a City record leaves their position or is no longer able to access their account.

### **C. Best Practices for Electronic Storage**

Before a department uses any online system to store City information, the Department of Information Technology must first consider the confidentiality, integrity, and availability of the system. San Diego Admin. Reg. 90.63 § 4.1.1(a). In addition, all City departments must follow state law regarding best practices for storing and maintaining records. SDMC § 22.2606 (incorporating Cal. Gov’t Code § 12168.7 which identifies applicable international standards); San Diego Admin. Reg. 85.10 § 2.7.2. These best practices include the requirement that only a “trusted system<sup>4</sup>” may be used for electronic document storage of public records.

For this reason, any contractual agreement with the service provider should ensure that the provider is obligated to maintain the integrity of the document storage system. This agreement should also allow the City to independently access any information stored by its employees in their scope of work and ensure that records generated by former employees remain accessible for their entire retention period. *See* San Diego Admin. Reg. 90.63 § 4.1.2.

## **III. Disclosing Electronic Communications**

Online collaboration tools must be used in a manner that complies with the City’s duty to respond to CPRA requests.

### **A. California Public Records Act**

The CPRA requires that public records be disclosed to interested parties, upon request, unless there is a specific legal reason not to do so. Public records include “any writing containing information relating to the conduct of the public’s business prepared, owned, used, or retained by

---

<sup>4</sup> A “trusted system” is defined as “a combination of technologies, policies, and procedures for which there is no plausible scenario in which a public record retrieved from or reproduced by the system could differ substantially from the public record that is originally stored.” Cal. Gov’t Code § 12168.7(c)(1).

any state or local agency regardless of physical form or characteristics.” Cal. Gov’t Code § 6252(e). Furthermore, “[e]mployees’ communications about official [City] business may be subject to CPRA regardless of the type of account used in their preparation or transmission.” *City of San Jose v. Superior Court*, 2 Cal. 5th 608, 616 (2017).

Under the CPRA and related case law, the format of the record and the nature of the platform hosting the record are generally irrelevant in determining whether a document is a public record. Because the City’s requirements under the CPRA are broadly interpreted to favor disclosure, City employees must ensure that the records they create (regardless of format or hosting server) are properly preserved according to the RDS and available to the department’s records coordinator when needed to respond to a CPRA request.

Because data hosted on outside platforms may not be readily available to the City when performing routine searches for public records, this can present logistical challenges in responding to CPRA requests. City employees should coordinate with their department’s “PRA Liaison” to ensure that relevant online collaboration tools are properly searched in response to record requests and that all response records are produced. San Diego Admin. Reg. 95.21 §§ 5.3, 5.4, and 6.1.1.

#### **IV. Remedies for Non-Compliance**

Remedies against employees who fail to comply with records retention and CPRA requirements can be severe. In addition to City disciplinary remedies, an employee could face civil penalties (SDMC § 12.0301), or even criminal prosecution for destruction of public records (Cal. Gov’t Code § 6201; SDMC § 12.0201). In addition, the City could face penalties, including payment of attorney’s fees (Cal. Gov’t. Code § 6259(d)) and court-ordered sanctions for discovery violations (Cal. Civ. Proc. Code § 2023.030).

### **CONCLUSION**

While online collaboration tools may facilitate communication among City employees, care must be taken to ensure that these tools comply with state law and Municipal Code requirements. Each department, in conjunction with the Department of Information Technology, must provide a secure system for City records to be organized, controlled, and stored so that they are properly retained and can be quickly identified in response to a request for public records. Entering into a master contractual agreement with the service provider may be advisable to ensure continued access and security. Furthermore, all employees who use these tools must understand their legal duties regarding records hosted on these platforms and be mindful of the significant remedies for non-compliance with applicable regulations.

Kris Michell, Chief Operating Officer  
Ron Villa, Assistant Chief Operating Officer  
Jonathan Behnke, Chief Information Officer  
October 9, 2019  
Page 6

Finally, departments should regularly review and revise City regulations, such as Administrative Regulations governing use of information technology and records retention, to ensure that they are up to date with current technologies.

MARA W. ELLIOTT, CITY ATTORNEY

By /s/ Eric S. Pooch  
Eric S. Pooch  
Deputy City Attorney

ESP:sc  
MS-2019-24  
Doc. No.: 1976767\_6

cc: Honorable Mayor and City Council  
Aimee Faucett, Chief of Staff, Office of the Mayor  
Andrea Tevlin, Independent Budget Analyst  
Kyle Elser, Interim City Auditor  
Elizabeth Maland, City Clerk