FYi

From the Information Policy Analysis Division

Volume 11 Issue 3
Summer 2012

Digital information meets data practices: Can I delete that email?

As technology continues to change the way government does its work, new questions always arise on how certain technology interacts with the Minnesota Government Data Practices Act (Minnesota Statutes, Chapter 13). Here is some practical advice for government entities in creating and maintaining email.

Don't treat every email the same! As you'll see from the following suggestions, entities should consider the content of an employee's email when responding to data requests or determining how long to keep them.

Understand and identify what is an *official record*. According to the "Official Records Act" (Minnesota Statutes, section 15.17), government entities are required to "make and preserve all records necessary to a full and accurate knowledge of their official activities." Employees should work with their supervisor, manager, responsible authority, or data practices compliance official to understand what types of emails may be considered an official record. An email from a grantee about equipment purchases, for example, may be an official record. It is important to remember that although any work-related email is government data, not all email is an official record that an entity is required to keep.

Be lean and efficient with use of email. There are generally three categories of work-related email.

1. Email that contains data considered to be an official record.
2. Email that serves an existing purpose for an employee to perform his/her work or for an entity to serve its customers, but not an official record.
3. Email that are not part of an official record and no longer serves a useful work purpose.

Email in category 1 should be kept according to the entity's records retention schedule. Email that fit categories 2 and 3 are government data, but not official records, and should be deleted when they no longer serve a useful work-related purpose.

Continued on page 2.

Inside this issue:

Information Policy Analysis Division

Admin Minnesota
DEPARTMENT OF ADMINISTRATION

Can I delete that email...cont.

Have policies in place to respond to data practices requests. Generally speaking, all email sent/received by government employees within the scope of their employment is subject to Chapter 13. Statutory requirements for responding to data requests include the following :

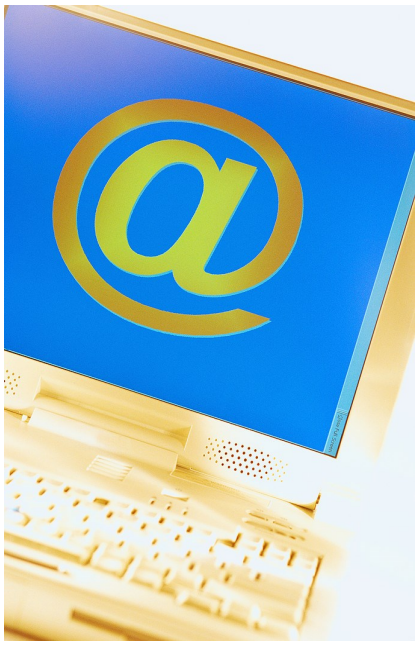
- Email must be kept in a manner easily accessible for convenient use (see Minnesota Statutes, section 13.03, subd. 1).
- Email that contains not public data must be protected from unauthorized access (see Minnesota Statutes, section 13.05, subd. 5).
- Entities must respond to requests for email containing public data in an appropriate and prompt manner and within a reasonable time (see Minnesota Statutes, section 13.03, subd. 2(a) and Minnesota Rules, part 1205.0300).

Do you have a personal use policy? While most email used by government entity employees is government data, email of a personal nature may be exempt from the requirements of Chapter 13 if the entity has a policy to allow for the limited use of government email accounts for personal use (see advisory opinion 01-075). For example, an email reminder to the employee's spouse to pick up milk.

Ensure proper redaction of emails. In responding to a data request, entities may find that certain email contains both public and not public data. Entities must make sure they properly redact any not public data in email in response to a data request.

Create a consistent policy on charging for copies of email. Entities may charge the actual cost for providing email in electronic form (i.e. forwarding an email). If an entity prints email in response to a request, it may charge **25 c**ents per page up to 100 pages and the actual cost for copies over 100 pages. Remember that a requester may always inspect data for free. See http://www.ipad.state.mn.us/docs/copycost.html for more information about charging for copies.

Ask if you need help. Be sure to consult with your entity's responsible authority, data practices compliance official, records manager, or legal counsel as necessary with questions about email content, keeping email, and providing email in response to a request. You may always contact IPAD at (651) 296-6733 or at info.ipad@state.mn.us.



Coming soon!

Look for information in upcoming days about IPAD's newest workshop:

The Do's and Don'ts of Government Personnel Data

Advisory opinion highlights

Drainage project "ditch viewers" not subject to OML

Opinion 12-011: A gathering of "ditch viewers" appointed by a Watershed District Board (drainage authority) pursuant to Minnesota Statutes, Chapter 103E, is not subject to the Open Meeting Law (Minnesota Statutes, Chapter 13D). The ditch viewers are not a separate public body subject to the OML, and given the nature of the viewers' statutory duties, they are also not a committee, subcommittee, board, department or commission of the Board. The Board appoints the viewers, whose duties and responsibilities are described in statute, but it has the final authority to make determinations regarding any drainage project.

Donor to County cannot remain anonymous

Opinion 12-012: A County asked about the classification of the name and cancelled check of a donor to a County project who wished to remain anonymous. The Commissioner determined that the data are not classified under Minnesota Statutes, section 13.792, and are presumptively public. The Commissioner also commented that, given some of the data relate to the donor's checking account and bank routing numbers, the County might want to consider whether those data might be classified under

Data about a program and personnel under criminal investigation, disciplinary data about an employee

Opinion 12-013: The Commissioner determined that an entity appropriately denied a request for access to all data about a particular program, including data on employees who participated in the program, because the program as a whole is under active criminal investigation, pursuant to Minnesota Statutes, section 13.82, subdivision 7, and the data are therefore classified as confidential/protected nonpublic.

The requester also asked for access to "Statements of Charges," referred to in public memoranda, to the extent they contained the specific reasons for, and data that document the basis of, final disciplinary action the entity took against an employee. (Minnesota Statutes, section 13.43, subdivision 2(a)(5).) The Commissioner opined that because the memoranda refer to the employee's actions as "outlined in the Statements of Charges," and given the entity's description of the data contained therein, at least some, if not all, of the data in the Statements are public.

Caselaw update

In ***Senne v. Village of Palatine***, ___F.3d ___ (7th Cir. 2012), [No. 10-3243 (7thCir. August 6, 2012)], the plaintiff alleged a violation of the Drivers' Privacy Protection Act (DPPA) after local law enforcement placed a parking citation on his car. The citation was in full view of the public and included the following personal data about the plaintiff: his full name, address, driver's license number, date of birth, sex, height and weight. (The printed citation also doubled as an envelope, with the personal information displayed on the outside.) The case was dismissed at District Court. The Court of Appeals reversed and remanded, holding that the respondent's placement of protected personal information in view of the public constituted a disclosure regulated by the DPPA, regardless of whether the plaintiff could establish that anyone actually viewed it.