NUMBER 24
REVISED SEPTEMBER 1998
1. ACCESS OVERVIEW
1.2

IPC
Practices

PUTTING ONTARIO'S INFORMATION AND PRIVACY LEGISLATION TO WORK
INFORMATION AND PRIVACY COMMISSIONER/ONTARIO
ANN CAVOUKIAN, Ph.D., COMMISSIONER

Q's and A's for Managing Electronic Mail Systems

The "questions and answers" below offer ideas to assist government organizations to effectively manage electronic mail (e-mail) documents, for purposes of the *Freedom of Information and Protection of Privacy Act* and *Municipal Freedom of Information and Protection of Privacy Act* (the *Acts*).

What is "E-mail?"

"E-mail" means an automated system that is used to create, send, and receive messages and other documents, from computer to computer. While the components of e-mail systems can vary, the discussion of e-mail systems here broadly includes all documents that can be created and transmitted in an e-mail program — including calendars and task lists, as they too could be subject to the *Acts*.

Are e-mail messages and other documents created in e-mail systems, records under the *Acts*?

According to the *Acts*:

"record" means any record of information however recorded, whether in printed form, on film, by electronic means or otherwise and includes:

(a) correspondence, a memorandum, a book, a plan, a map, a drawing, a diagram, a pictorial or graphic work, a photograph, a film, a microfilm, a sound recording, a videotape, a machine-readable record, any other documentary material, regardless of physical form or characteristics, and any copy thereof; and

(b) subject to the regulations, any record that is capable of being produced from a machine-readable record under the control of the institution by means of computer hardware and software or any other information storage equipment and technical expertise normally used by the institution.

E-mail created or received by government employees in connection with official government business, is subject to the *Acts*. E-mail documents are subject to the same legal obligations, policies, rules, directives, and legislation/regulations as are paper documents. They should be included in record retention schedules and managed in a way that is consistent or common with existing record management systems and file classifications.

The same decision-making process that determines record or non-record status should be applied to messages and documents created in e-mail systems. The *Acts* do not distinguish by medium or format — it is the content that determines what *is* and what is *not* a record.

Whose job is it to figure out how "the who-what-when-where and how" e-mail messages and documents should be managed?

Although all organizations will operate differently, what is needed is a plan. Ideally, freedom of information and privacy co-ordinators, record managers, system administrators/local area network operators and end users should co-operatively assess/plan organizational needs and determine responsibilities for the effective management of e-mail systems.

How should e-mail records be managed?

An ideal electronic records management system for e-mail documents, for purposes of the *Acts*, may be a stand-alone scheme for e-mail documents only, or, may incorporate all electronic records together within one record keeping system — that is, an electronic system in which records are collected, organized, and categorized so that their preservation, retrieval, use, and disposition are facilitated. Look for software applications that permit an electronic record keeping system to:

- Manage an electronic repository of records that is untamperable, indexed and searchable;
- Allow for reasonable search and easy retrieval for multiple authorized users at all times;
- Identify and group/link e-mail records and attachments according to established record-keeping systems and statutory requirements; and
- Securely retain information for the required retention schedule.

How can I manage my electronic records?

Ongoing instruction should be given and policies should be devised and provided to government personnel on the appropriate use of government computer equipment. Training and awareness on how to follow proper electronic record keeping should be provided to all government personnel who use e-mail systems.

Can I keep my e-mail messages in my personal directory?

As a minimum measure, e-mail messages that relate to current or ongoing projects/programs could be systematically organized, for example, by topic or project, into folders or envelopes by the creator or receiver of the e-mail message and kept in one's personal directory.

A preferred practice would be to electronically transfer and deposit the documents subject to the *Acts*, into an indexed, searchable, secure and untamperable repository. Access to this repository should be restricted to those individuals who are authorized and have a legitimate business need for the information.

What should my organization consider when purchasing software or undertaking a system upgrade?

Although the electronic management of e-mails is in its infancy, this is the ultimate goal. In the future, as software is upgraded or purchased new, the ability to address the electronic manageability of e-mail, such as an electronic record keeping system, should be one of the selection criteria. Although no present software will meet this criteria now, hopefully a system will be developed to manage e-mails along with other electronic files.

Another factor to consider is that existing e-mail documents should be migrated to new versions or upgraded systems when changes occur. If electronic conversion cannot occur, then hard copies should be prepared and filed. Avoid situations where records are retained but then cannot be read later on because of a new/upgraded system.

For the purposes of the *Acts*, what should a good electronic record keeping system be able to do?

Overall, the search and retrieval of responsive e-mail documents should be quick and easy for multiple authorized users. An electronic record keeping system that provides for designating (or tagging) and linking e-mails and all related documents and/or attachments as records, should be considered.

An electronic record keeping system should be able to search for documents within a certain time frame, by a particular topic or key words, created by a particular individual.

An electronic record keeping system should have the ability to recognize and identify when an e-mail record may be deleted, transferred to a records centre or if appropriate, to the Archives.

Authorized users should be able to search, find, view, and print the document for as long as it needs to be officially retained. E-mail documents containing personal information need to be retained for a minimum of one year.

What is contextual information, and is it important?

Contextual information is important. Without it, an e-mail document may have no value as a record. With paper, the context (date, addressee, author, company names, etc.) of the information is obvious. With an e-mail this information is not necessarily obvious.

Contextual information such as transmission and receipt data should be retained along with the text of the e-mail message. Transmission data and receipt data should include: the true names (not aliases or "nicknames") of the sender and all recipients; the true names of individuals who received carbon copies and blind carbon copies; a date of when the message was sent and/or received; and perhaps, if desired, the time the message was sent.

What about severing, changing or correcting an e-mail message or document?

The original electronic record should be preserved. Changed or revised or subsequent documents should be designated as new, dated, linked to the original and all other related documents, and be recognizable as a version. The version should always be discernable when locating, viewing, retrieving or producing the e-mail document. The date on each document should remain constant without being changed when accessed, read, copied or transferred.

Are network backup tapes a reasonable and reliable way to retrieve deleted e-mail messages?

It depends on the type of system you have. If retrieval is quick, reliable and inexpensive, then it may be possible to use backup tapes (including contextual information). If not, then backup tapes should be done regularly for disaster recovery, and not for record retrieval purposes under the *Acts*.

Are there other rules or directives or guides to follow?

- Management Board Secretariat's Directive and Guideline 7-3 on *Information Technology Security* details the mandatory requirements for provincial government organizations to achieve information technology security. Both the Directive and the Guideline could also be of assistance to municipal government organizations. Note that Appendix B of the Guideline provides a "Security Assessment Questionnaire."
- See also, other Management Board Secretariat guidelines and directives. For example, *Directive 7-5: Management of Recorded Information* and *Directive 7-9: Records Management*.
- Archives of Ontario has produced a series of fact sheets on Recorded Information Management (RIM). Of special interest would be: RIM Fact Sheet # 5 - *Electronic Records: Some Key Challenges*; RIM Fact Sheet #6 - *Electronic Documents: Filing Fundamentals*; and RIM Fact Sheet # 7 - *Electronic Records: What About E-Mail?*;
- For a discussion of privacy issues and electronic mail systems see the IPC's papers — *Privacy Protection Principles for Electronic Mail Systems*, February 1994; and *Electronic Records: Maximizing Best Practices.*

What about future developments?

The ever-expanding world of the Internet can vastly enable more open government through on-line access to government-held general records and through encrypted e-mail communication between the public and government officials. From a customer service perspective, electronic service delivery is desirable because it can be fast, cheap, and convenient.

IPC
Practices
is published regularly by the **Office of the Information and Privacy Commissioner**.

If you have any comments regarding this publication, wish to advise of a change of address or be added to the mailing list, contact:

Communications Department
Information and Privacy Commissioner/Ontario
80 Bloor Street West, Suite 1700
Toronto, Ontario M5S 2V1
Telephone: (416) 326-3333 • 1-800-387-0073
Facsimile: (416) 325-9195
TTY (Teletypewriter): (416) 325-7539
Web site: http://www.ipc.on.ca

50% recycled paper, including 20% post-consumer fibre

ISSN 1188-7206