foip bulletin

Number 12 | Revised March 2009

E-Mail: Access and Privacy Considerations

CONTENTS

INTRODUCTION

E-mail is an essential communication tool for public bodies. As records, e-mail messages are subject to both the access and protection of privacy provisions of the *Freedom of Information and Protection of Privacy Act* (the FOIP Act). E-mail messages held by government ministries are also subject to the Records Management Regulation.

Because of its special versatility, and the way it is perceived by staff, e-mail can present certain challenges for the administration of access and privacy legislation. For example, e-mail may, on different occasions, serve the function of a telephone call, a memo, a circular, or a meeting. It can be simply a method of transmitting a document for local printing (like a fax), or it can take the place of a different kind of record (e.g. meeting notes). Staff can blur these familiar distinctions further by combining a number of these different functions in a single message.

As a result, some e-mail has characteristics that make staff uncomfortable about the prospect of disclosure in response to an access request. For example:

- e-mail may lack the formality of other records on the same subject;
- the writing and presentation may not be very polished;
- it may be more conversational, perhaps more candid or less neutral in tone than would be the case in other forms of communication;
- it may have personal content on non-work-related matters.

The functionality of e-mail systems, which allows users to compose, transmit and receive messages almost instantly across networks, is part of the value of e-mail, but it also has consequences for both access and privacy protection. For example, the ability to easily send or forward an e-mail message to multiple recipients can result in multiple copies of the same record residing in many different locations. It can also result in the inadvertent disclosure of personal information.

The technology that supports the e-mail system can also create a risk of unauthorized disclosure of information. There are significant differences between the security of e-mail sent within a local area network and e-mail sent via the Internet or wireless technologies. Although the security of different networks is not always well understood by users, the person responsible for compliance with the FOIP Act within a public body needs to have an understanding of the public body's e-mail environment to ensure that adequate privacy protection measures are in place. For this reason, it is a good practice for the FOIP Coordinator to be aware of all of the e-mail systems being used by public body employees and to be involved in the planning of changes to e-mail.

This FOIP Bulletin is intended to assist public bodies in complying with their obligations under the FOIP Act by highlighting the access and privacy protection issues raised by e-mail. It does not address other management issues relating to e-mail, such as records management, e-mail monitoring or the development of a general policy on the use of e-mail. Information regarding these issues is available in the *Guide to Managing Electronic Mail in the Government of Alberta*, which is published on the Records and Information Management website at www.im.gov.ab.ca.

Public bodies are also employing instant messaging (IM) systems, which have the capacity to duplicate and expand upon the functionality of e-mail. This FOIP Bulletin does not specifically address a public body's obligations under the FOIP Act with respect to records generated by the use of IM systems. However, public bodies that collect, use or disclose personal information, conduct business transactions, or make business decisions using an IM system should be aware that many of the same access and privacy considerations of e-mail may apply. For guidance on other management issues relating to IM systems, such as records management, monitoring of use, or the development of a general policy on the use of instant messaging, see the Government of Alberta's *Managing Instant Messages* published on the Records and Information Management Information website.

Decisions, practice notes or publications issued by the Office of the Information and Privacy Commissioner of Alberta cited in this Bulletin may be found on the OIPC website at www.oipc.ab.ca.

DEFINITIONS

"**Employee**" in relation to a public body includes a person who performs a service for the public body as an appointee, volunteer or student or under a contract or agency relationship with the public body (**section 1(e)** of the FOIP Act).

"**Personal information**" means recorded information about an identifiable individual, including the individual's name, home or business address or home or business telephone number, an identifying number, symbol or other particular assigned to the individual, anyone else's opinions about an individual, and the individual's personal views or opinions, except if they are about someone else (see **section 1(n)** of the FOIP Act for the complete definition). In *Order 2000-032*, the Information and Privacy Commissioner ruled that e-mail addresses are personal information.

"**Record**" means a record of information in any form and includes notes, images, audiovisual recordings, x-rays, books, documents, maps, drawings, photographs, letters, vouchers and papers and any other information that is written, photographed, recorded or stored in any manner, but does not include software or any mechanism that produces records (**section 1(q)** of the FOIP Act).

"Thread" in the context of e-mail means a series of messages that have been sent as replies to each other. By reading each message in a thread, one after the other, one can see how the discussion has evolved. A new thread in a discussion can be started when an individual sends a message that is not a direct reply to an earlier message.

PROCESSING AN ACCESS REQUEST INVOLVING E-MAIL

Processing an access request that involves e-mail is similar in most respects to processing any other access request. The same principles apply. However, some of the special characteristics of e-mail need to be taken into consideration to ensure that a public body's response to the request is accurate and complete.

The FOIP Act requires a public body to "make every reasonable effort to assist applicants and to respond to each applicant openly, accurately and completely" (**section 10(1)**). Part of this duty to assist the applicant involves performing an adequate search. The Commissioner has said that, to perform an adequate search, a public body must make a reasonable search of all locations where records relevant to the request might be located (see *IPC Order 99-021*). This includes locations where e-mail that is in the custody or under the control of a public body is stored.

Scope of the search

Program areas are normally responsible for locating and retrieving all records relevant to a request. The following guidelines may assist program areas in completing the e-mail component of the search.

A search must include all relevant e-mail messages in the custody or under the control of the public body.

The FOIP Act establishes a right of access to "any record in the custody or under the control of a public body" (**section 6(1)**). Since "record" is defined in the Act as "a record of information *in any form*" (**section 1(q)**), an applicant has a right of access to all e-mail messages in the custody or control of the public body, subject only to the exceptions in the Act.

- **The search must include relevant e-mail on all servers, hard drives and personal storage devices in the custody of the public body, as well as any printed hard copies.**

A record is in the "custody" of a public body if it is in the public body's possession (*IPC Order 2000-005*). This would be the case for any e-mail residing on a server owned by a public body, or on another local storage medium, such as an individual employee's computer hard drive. This would also include any paper versions filed centrally or in individual offices.

- **The search must include relevant e-mail that is under the public body's control, regardless of where the e-mail is stored.**

A record is in the "control" of a public body if the public body has the authority to manage the record, including restricting, regulating and administering its use, disclosure or disposition. The Commissioner considered some of the indicators that a record may be in the control of a public body in *Order 99-032*. Some examples of e-mail that would likely be deemed to be under the control of a public body are:

– e-mail residing on an external server used by a public body under a contractual arrangement

– e-mail sent or forwarded to or from an employee's personal e-mail account with a commercial Internet service provider (ISP), if the content of the e-mail relates to the public body's mandate and functions

  e.g. work-related e-mail in an employee's webmail account

– e-mail created by a person in the performance of a service for a public body as a volunteer or student or under a contract (as noted above, these are all considered "employees" of the public body), regardless of where the e-mail is stored

  e.g. e-mail sent by a contractor to a client if the e-mail relates to the service being performed for the public body

– e-mail stored on a computer owned by a public body and residing in the home of an employee of a public body, whether that employee sends and receives e-mail through a commercial ISP or through a remote connection to a public body's mail server, or accesses the public body's e-mail system through a virtual private network (VPN)

  e.g. e-mail exchanged between an employee working from home and a contractor through one or more commercial ISPs, but not e-mail covered under a private use agreement

The Commissioner has not yet considered whether a public body has custody of data not physically in its control, as in the case of e-mail and data related to e-mail held by commercial ISPs or webmail applications, or data related to e-mail possibly held by providers of wireless hotspots (such as airports and hotels). This information is likely in the control of a public body only to the extent that the employee is able to access the e-mail message from his or her ISP or the webmail developer.

- **The search must include all responsive records, including any responsive "personal" e-mail.**

Most access requests are expressed in relation to a particular subject. However, a request may be worded in such a way as to include e-mail that an employee would regard as "personal." This might be the case if an applicant asked for all the incoming e-mail of a named individual that was received between specified dates.

In such a case, a FOIP Coordinator would clarify with the applicant whether e-mail of a personal nature should be included. If the applicant did intend to include personal e-mail within the scope of the request, the public body would be required to include the personal e-mail in the responsive records. The public body would then have to rely on other provisions in the Act to limit the applicant's access to the employee's personal information.

Non-responsive personal content of an otherwise responsive e-mail message is discussed below (see "Identifying responsive e-mail records").

- **The search must include deleted e-mail that has been moved to a "trash folder" but has not been permanently deleted.**

If e-mail has simply been moved to a "trash" folder within the e-mail system, it has not been permanently deleted. E-mail that can easily be restored from the trash should be searched and any responsive e-mail produced.

- **There may be a requirement to search back-up tapes, depending on the circumstances of the case.**

In *Order F2007-028*, the Commissioner ordered a public body to conduct a search of the public body's computer back-up system.

In this case, an applicant requested access to all information regarding him held by a public body, including all paper and electronic records, on-line and off-line, archived, held, received or distributed during a specified time period. Upon being advised by the public body that it would not conduct a search of its back-up media, the applicant complained to the Commissioner that the public body had not completed a search of all of its electronic records, and in particular, that the public body had not conducted an "offline search of email transmissions."

The Commissioner found that the public body did not make every reasonable effort to assist the applicant as required under **section 10,** as the public body did not conduct an adequate search (*IPC Orders 97-003, 97-006, 2001-016*). An adequate search requires a public body to make every reasonable effort to search for the actual record requested and inform the applicant in a timely fashion about what has been done (*IPC Order 2001-016).*

The public body established that back-up tapes existed for a portion of the time period outlined in the applicant's request, but that it did not search these tapes. Though the public body noted that its technology department occasionally searched back-up electronic records for law enforcement purposes, it had decided not to conduct a search in this case because it would be expensive, difficult and time consuming to do so. The Commissioner rejected the public body's argument for not conducting the search, stating that if a public body were able to refuse to search on these grounds, the effect would be to render an applicant's rights of access under **section 6** effectively meaningless and defeat the purpose of access to information legislation. The Commissioner held that the Act recognizes that it can be costly and time consuming for a public body to conduct searches, which is why public bodies can charge fees under **section 93** and extend time limits for responding under **section 14**. The Commissioner believed that the public body was attempting to disregard a significant portion of the access request, even though the circumstances did not meet the requirements of **section 55**.

The Commissioner found that the applicant had provided sufficient detail for the public body to identify the records he was seeking. In addition, as the public body had located e-mail records in the computer system that fell within the scope of the access request, it was likely that related electronic records would exist within the back-up files as well.

The Commissioner also stated that to establish that a search for records was adequate, the head should have direct knowledge of the steps taken to search for records. The head of the public body did not provide

satisfactory evidence of the steps the public body took to locate records among the records it chose to search.

The Commissioner noted, however, that there may be situations where a public body is unable to search or access electronic back-up records. In such cases, the public body may establish that it has performed an adequate search for records without searching those records. However, the evidence of the public body in this case was that it had the ability to access and search back-up records, but had chosen not to.

An Adjudicator also requested a review of back-up tapes and other media used for the purposes of business continuity and disaster recovery, or for archival purposes, during a review (*IPC Order F2005-005*).

Identifying responsive e-mail records

The program area will normally be responsible for determining which e-mail is relevant to the request and for submitting copies to the FOIP Coordinator. The following directions may assist program areas with providing responsive records to the Coordinator.

- **Provide hard copies of all e-mail that is "reasonably related" to the subject of the request.**

The Commissioner has said that a record is responsive to a request if it is "reasonably related" to the request (*IPC Order 97-020*). A public body may treat portions of a record as non-responsive only if they are clearly separate and distinct and entirely unrelated to the access request (*IPC Order 99-020*).

If an e-mail message that is generally responsive to a request has clearly separate personal content (e.g. a postscript containing arrangements for some social activity), it may be allowable to treat the separate personal information as non-responsive. If the personal content is not clearly separated, it will have to be severed in accordance with the Act's exception for personal information.

Since forwarding e-mail to the FOIP Coordinator through the e-mail system would actually create a new record, it is generally more practical for e-mail to be submitted in hard copy.

- **Ensure that an expert in the subject area assists in a thorough search of the e-mail system and can provide documentation on the search strategy used.**

The Commissioner has said it is insufficient to use a limited keyword search to attempt to locate responsive records (*IPC Order 99-002*). An adequate search requires more than a search for a keyword in an e-mail subject line. The subject-line text may have been an accurate description for the first message, but may not reflect the scope of the subject matter as the thread of the discussion has developed. A knowledgeable employee in the program area should be able to define an appropriate search strategy that takes the special characteristics of e-mail into consideration.

- **Review any attachment to a responsive e-mail message for relevance to the request. Provide a hard copy of any responsive attachment.**

If an e-mail record is responsive to a request, any attachment is likely to be considered potentially responsive and should be reviewed for relevance. If an attachment is not considered responsive, this should be explained.

- **Review all e-mail records in any "thread" that includes a relevant message. Provide all responsive records, including partial duplicates.**

Multiple e-mail records may be generated in the process of an exchange on a particular subject. In some cases, the individual contributions may be accumulated in a "thread" (see "Definitions" above). If the matter discussed in the e-mail exchange is relevant to the applicant's request, it is likely that a record containing an entire thread would be considered responsive to the request.

All the e-mail generated at each stage of the exchange might also be considered responsive (e.g. an e-mail message, including all of the exchange to date, sent to multiple recipients, and the reply, again including all of the exchange to date, sent to multiple recipients). This may mean there are some records that are not duplicates, but which exactly duplicate parts of the most complete record.

The program area should provide *all* responsive records, even if this involves some duplication of

information. If the request involves a lot of e-mail, and it would not place an unreasonable burden on the public body, the FOIP Coordinator might find it helpful to clarify with the applicant whether it is sufficient to supply the smallest number of records needed to accurately represent the exchange and provide the complete thread.

If the applicant and the public body agree to this option, the public body must ensure that the message contents are in other respects genuine duplicates (e.g. that information has not been altered or deleted when an individual replied to a message or forwarded it).

- **Ensure that transmittal data is included. If a message is sent to a group or list, include information about the list.**

The public body must ensure that the record shows who sent and received each message and when, as well as who received a copy (since the transmittal data will differ on each copy of the message).

Information regarding e-mail recipients may not be available if the e-mail is sent to a group or a list identified by a list name in the transmittal data. It is unlikely, for example, that the system will preserve older versions of an updated list. A public body is not required to reconstruct non-current lists.

- **Review the e-mail transmittal data for possible related threads.**

When searching for responsive e-mail, the list of recipients to whom the e-mail was sent or copied may suggest additional locations of responsive records. For example, a recipient may not have responded to the sender but may have forwarded the e-mail to other individuals who were not included in the original list. This may have generated another separate thread of related e-mail. When considering the pool of recipients, it should be remembered that an e-mail message will include the names of recipients of blind copies in the sender's transmittal data.

- **Ensure that employees understand that, once a FOIP request has been received, no relevant e-mail may be deleted from the e-mail system.**

It should be explained to employees that intentional alteration or destruction of a record for the purpose of evading an access request is an offence under the FOIP Act (**section 92(1)(e), (g)**). Employees should also be advised that e-mail systems have audit functions to enable the network administrator to identify modification or deletion of messages. In addition, there is often a copy of a deleted e-mail message in another user's mailbox.

No record, including a transitory record, that may be responsive to an active FOIP request may be deleted until after the request has been processed and any time limit on the right of review has passed. (Transitory records concerning the subject of the request that post-date the request can continue to be deleted according to standard practices.)

- **The public body may be required to provide the e-mail record in electronic form.**

Order F2002-017 discussed the requirement to disclose a record in electronic form. In that Order, the Adjudicator said that **section 10(2)** requires a public body to create a record in its original form if doing so would not unreasonably interfere with the public body's operations. The Adjudicator found that the public body should provide an electronic copy of e-mail records, if requested to do so by the applicant and if the public body has the ability to do electronic severing. In this case, electronic severing was not possible and the e-mail records were disclosed in paper form.

Applying exceptions

Applying the Act's exceptions to disclosure should be similar for paper and e-mail records, since the exceptions relate to the content of the message rather than the medium. However, there are a few points to bear in mind.

The most important concerns the manner in which a public body routinely handles sensitive information. A number of exceptions in the FOIP Act refer to information supplied in confidence:

- business information (**section 16(1)(b)**),
- personal information (**section 17(5)(f)**),
- evaluative or opinion material regarding an employee (**section 19(1)** and **(2)),**

- information in a correctional record (**section 20(1)(n)**),
- government information (**section 21(1)(b)**), and
- information subject to legal privilege (**section 27(1)(a)**).

A public body wanting to apply these exceptions to e-mail may be required to demonstrate that the information has been treated in a secure manner during transmission over the Internet. A standard confidentiality message attached to all e-mail would be less persuasive than, for example, the use of encryption in accordance with an established policy.

When considering the application of exceptions, it needs to be noted that transmittal data in an e-mail message may include personal information to which the Act's exception for third party personal privacy (**section 17**) applies. Although an e-mail address is not specifically listed in the Act's definition of "personal information" (**section 1(n)**), it is personal information if it can be related to an "identifiable individual." For example, joe.smith@gov.ab.ca would be considered personal information, whereas foiphelpdesk@gov.ab.ca would not.

If third party personal information is involved, the public body must consider whether disclosure may be an unreasonable invasion of privacy under **section 17**. If **section 17** may apply and the public body is intending to disclose the information, it will be necessary to provide notice to the third party (under **section 30(1)(b)**).

E-mail is often sent or copied to multiple recipients and retained in multiple locations. If an applicant sends similar requests involving related e-mail records to two or more public bodies, it may be helpful for the FOIP Coordinators to consult to ensure that each public body has located all the responsive e-mail records.

PROTECTION OF PRIVACY

E-mail messages may contain a wide range of different kinds of personal information, which must be protected under the FOIP Act. An e-mail address which can be linked to an identifiable individual is personal information (see "Definitions" above). Although e-mail poses some particular challenges for the protection of privacy, the same general principles that apply to paper records with respect to the collection, use, disclosure, and protection of personal information also apply to e-mail.

Collection of personal information

Collection of personal information may occur by means of e-mail in a variety of circumstances.

For example, a web page may have an e-mail address that the public can use to send a question to the public body. An individual is not required to provide any personal information other than an e-mail address, which is automatically attached to the message. However, an individual may volunteer personal information in the course of asking a question or making a comment.

Once the public body has received the inquiry, it has collected the personal information, and the e-mail record is in the custody or control of the public body. This means that the personal information is subject to all the privacy provisions of **Part 2** of the Act, including the requirement to protect the information, and restrictions on use and disclosure.

The public body must provide notice of collection under **section 34(2)**. A public body must inform the individual of the purpose for which the information is collected, the specific legal authority for the collection, and the title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection.

Use and disclosure of personal information

Personal information may be used for the purpose for which it was collected, or for a consistent purpose (**section 39(1)(a)**). The personal information may be used only to the extent necessary to enable the public body to carry out its purpose in a reasonable manner (**section 39(4)**).

Applying this provision to e-mail web inquiries, the personal information may be used for the purpose of replying to the query or to take some action in response to the query. Normally it would not be used for other, unrelated purposes.

It is very easy to forward e-mails, even to groups of people, within or outside a public body. Users need to be aware that forwarding an e-mail containing personal information must be a permitted use under **section 39** or a permitted disclosure under **section 40** of the FOIP Act.

Under **section 40**, personal information can be disclosed for certain purposes. For example, personal information can be disclosed for the purpose for which the information was collected or for a consistent use under **section 40(1)(c)**.

Personal information can be disclosed to a fellow employee under **section 40(1)(h)**, if the information is necessary for the performance of the employee's duties. For example, the recipient of the e-mail may forward the message to an employee in the program area for a reply.

Personal information can also be disclosed to an employee of another public body, if disclosure of the personal information is necessary for the delivery of a common or integrated program or service, and is also necessary for the performance of the employee's duties (**section 40(1)(i)**).

All disclosures are subject to **section 40(4)**, which limits disclosure to what is necessary to enable the public body to carry out its purpose in a reasonable manner. In *Order F2005-014*, the Adjudicator found that the President of a public body improperly forwarded an entire e-mail thread to employees. The Adjudicator noted that the President should have sent only a single e-mail informing the employees of his decision and the reasoning behind it. The complainant's initial disclosure of the e-mails to the President was not a consent to forward the entire sequence of e-mails onward.

Employees should be careful not to disclose personal information if it is not needed. For example, an individual might send an e-mail message to a public body that provides services to persons with disabilities, saying that he or she is disabled and is trying to obtain assistance. The sender might also mention that the links from your website to another site are not working. The employee who receives the e-mail does not need to forward the message to the webmaster to enable the webmaster to fix the link.

A better privacy practice is to create a new e-mail, advising the webmaster that the link is broken. The webmaster does not need to know the personal information or the name of the sender.

When dealing with sensitive information, it is important to send e-mail to the correct recipient(s). This is particularly necessary if the message is being sent to a long distribution list or is being put on a listserv. E-mail users should:

- ensure that the correct e-mail addresses of recipients are used, and are typed correctly;
- avoid using the "reply to all" feature unless really necessary;
- verify that a distribution list or a listserv is up-to-date and that the recipients for a particular message are authorized to receive the message before sending it to the entire list or listserv;
- consider using a list name rather than individual names, or sending blind copies to individuals on a list, if the message discloses sensitive information about the recipients; and
- obtain the author's permission before forwarding his or her e-mail message to a discussion group, listserv, or newsgroup, or posting it on an electronic bulletin board.

Protection of personal information

Section 38 of the FOIP Act requires public bodies to protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, or destruction.

E-mail is vulnerable to both intentional and unintentional privacy breaches. E-mail messages intercepted during transmission can be used and disclosed in ways that can be very harmful to personal privacy. Some features of e-mail also heighten the risk of unintentional privacy breaches, which can occur within any network environment. For example, the ease with which one can forward a message or an attachment can lead to the disclosure of more personal information than is needed by the recipient to perform his or her duties.

In the mid-1990s, Ontario's Information and Privacy Commissioner suggested some general principles that public bodies could apply to address privacy protection concerns. Since that time, these principles have been widely adopted by public bodies and privacy practitioners. His recommendations to public bodies were:

- create an explicit policy which addresses the rights and obligations of e-mail users regarding the confidentiality of messages on the system;
- train users regarding the e-mail policy and the privacy and security issues surrounding the use of e-mail;
- do not use e-mail systems for collecting, using and disclosing personal information unless there are adequate safeguards to protect privacy;
- explore technical means of protecting privacy; and
- develop appropriate security procedures to protect e-mail messages.[1]

Technical security measures

There are significant differences between the security of e-mail messages sent within a local area network, and e-mail sent via the Internet. For example, when a Government of Alberta employee sends an e-mail to another government employee across the government network, the message travels within a secure system. When a public body uses a commercial Internet service provider, e-mail sent between employees is delivered via the Internet and there is a much higher possibility of interception.

It is important to note, however, that each Internet-based e-mail technology provides a different level of protection. The overall security of e-mails sent via the Internet varies depending upon the technology used to send the message and what, if any, security mechanisms are employed by users.

The most secure are virtual private networks. VPNs are private data networks built upon the shared public infrastructure of the Internet. VPNs use encryption and other security mechanisms and are highly secure, ensuring that only authorized users can access the network and the data cannot be intercepted by someone on the Internet. Encryption converts data into a form that is unintelligible to anyone without the "decryption key." Using a VPN, an off-site public body employee can securely access and use his or her public body's e-mail system and have a comparable level of security as though that employee were on-site. To logon using a VPN, users generally need to authenticate themselves using a special token such as a smart card or RSA SecurID token. Authentication ensures that the sender and recipient are who they claim to be.

Webmail applications generally include very basic levels of security and in some cases almost none. Commercial ISPs typically offer services that provide enhanced protection for e-mail that should be investigated for suitability. Third party software is also available that can encrypt and password protect documents.

E-mails are also sent using various wireless transmission technologies such as home and public networks, Bluetooth®, cell phones and personal digital assistants (PDAs). Like unsecured Internet based e-mail technologies, wireless-based technologies can be more susceptible to e-mail interception. However, in both cases, security can be improved where users employ encryption mechanisms.

In view of the risk of interception of e-mails, public bodies should consider whether it is appropriate to implement special security procedures or to place restrictions on the use of e-mail for the transmission of personal information via the Internet or wireless technologies. Users and public bodies should consult documentation that is provided with wireless devices or network hardware such as wireless routers.

When transmitting third party personal information via e-mail, consideration should be given to the adequacy of security safeguards and the use of safeguards such as encryption and authentication. Together these processes help to ensure that messages are read only by their intended recipients.

Public bodies should ensure that employees use at least some common security measures. For example, public bodies should require employees to use a

[1] Source: Tom Wright, *Privacy Protection Principles for Electronic Mail Systems*, 1994.

password while using the e-mail system or Internet. Employees should also ensure that their passwords are not shared, are hard to guess, and are changed regularly, or immediately if compromised.

Security practices should also include the use of password-protected screen-savers. Sensitive e-mail may need to be stored in protected directories where access is limited or restricted. Portable equipment containing personal information should not be left unattended. Users should take steps to ensure that the content of e-mails displayed on their screen is not readily visible to bystanders or so-called "shoulder surfers."

Government ministries must comply with the Government of Alberta *Policy for the Transmission of Personal Information via Electronic Mail and Facsimile*. This policy requires ministries to establish standards for the secure transmission of sensitive personal information. These standards will normally require the use of encryption and the authentication of the sender and recipient.

Security policies and directives produced by the Office of the Corporate Chief Information Officer of the Government of Alberta are published on the Records and Information Management website at www.im.gov.ab.ca.

The Records and Information Management website also publishes guidance on standards for the use of personal digital assistants: *Report on Securing PDA Devices: Best Practices* (Office of the Chief Information Officer, 2003) and *Managing Personal Digital* Assistants *(PDAs)* (Records and Information Management, 2005).

Other security measures

Before transmitting e-mail that contains third party personal information, the sender should try to remove all personal identifiers and should disclose only the minimum amount of personal information that is necessary to carry out authorized purposes.

Inclusion of a privacy statement in each message may provide some protection against secondary disclosure. Most government departments now automatically attach the following privacy/ confidentiality statement to all e-mail leaving the department:

> This communication is intended for the use of the recipient to which it is addressed, and may contain confidential, personal, and/or privileged information. Please contact us immediately if you are not the intended recipient of this communication, and do not copy, distribute, or take action relying on it. Any communication received in error, or subsequent reply, should be deleted or destroyed.

In *Investigation Report 2001-IR-001* concerning a breach of privacy caused by e-mail being sent to the wrong address, the Information and Privacy Commissioner of Alberta endorsed a number of recommendations regarding the protection of third party personal information contained in e-mail messages and systems.

The report recommended that:

- agreements with agencies or contractors include clauses that require them to protect personal information received from the public body, from unauthorized use, collection and disclosure;
- policies and procedures be in place that require employees and agencies or contractors to check directories and e-mail addresses on a continual basis to ensure the addresses are correct and current;
- agencies/contractors be required to confirm receipt of e-mail;
- agencies/contractors be required to establish clear policies for their employees regarding access, use and disclosure of personal information received from the public body; and
- agencies/contractors be required to conduct an assessment of risk associated with the use of Internet service providers.