IPC
Practices
NUMBER 20
REVISED SEPTEMBER 1998
PUTTING ONTARIO'S INFORMATION AND PRIVACY LEGISLATION TO WORK
INFORMATION AND PRIVACY COMMISSIONER/ONTARIO
ANN CAVOUKIAN, Ph.D., COMMISSIONER

Privacy and Confidentiality When Working Outside the Office

This IPC Practices *focuses on protecting records and ensuring the confidentiality of personal and confidential information while working outside a traditional office environment. The suggestions offered were jointly developed by a working group comprised of provincial and municipal Freedom of Information and Privacy Co-ordinators and the IPC. Not all of the suggested practices are required under the* Freedom of Information and Protection of Privacy Act *or the* Municipal Freedom of Information and Protection of Privacy Act (*the* Acts). *However, all of the suggestions represent good records management and promote the purposes of the* Acts.

Increasingly, employees are working from locations outside the traditional office setting. This manner of working is commonly referred to as teleworking. Teleworking may include any situation from case workers who make home visits to clients, to employees who occasionally take work home to complete an assignment, or who work from home on a regular basis. When teleworking, records may be removed from the office or created off-site. In addition, employees who telework often convey information and records through various means of technology. Teleworking raises concerns about the privacy and confidentiality of records.

Technology has had an impact on how records are handled and on how personal and other information is collected, stored, and communicated. Information may be stored electronically instead of on paper, or communicated via cellular phones, fax machines, voice mail, modems, or other means. While this technology is efficient, it may diminish the confidentiality of the information transmitted. For that reason, the IPC suggests that institutions encourage employees to take special care when using technology.

Employees who telework are responsible for protecting personal information and for ensuring the confidentiality and security of records in all formats (paper, computer, photos, drawings, recordings, etc.) Institutions subject to the *Acts* are encouraged to create a clear and well-communicated policy to assist employees who telework. The purpose of the policy is to ensure that the teleworking environment does not lead to inadvertent breaches of the *Acts*.

Creating a Policy

Institutions should consider the following suggestions for creating a policy specific to their needs and environment.

Suggestions

- Develop a record classification system that outlines the circumstances in which categories of records can, may, or should never be removed from the office.
- Contact the group within your institution responsible for information technology to ensure you are aware of current security practices.
- Refer to Management Board's Directive 7-3, "Information Technology Security," for guidance. This directive applies only to provincial institutions, but may be useful to local government institutions.
- Familiarize employees who use fax machines with the IPC's "Guidelines on Facsimile Transmission."
- Familiarize employees who use e-mail with the IPC's "Privacy Protection Principles for Electronic Mail Systems."

Considerations

- *Paper and electronic records*
  - Be familiar with existing records management practices in the office.
  - Consider the privacy provisions of the *Acts*.
  - Consider the confidentiality of records subject to the *Acts*' exemptions to access, particularly those that are mandatory.
  - Incorporate the highest level of security appropriate to the format of a record. For example, when transporting records or diskettes, keep them in a locked or secure briefcase, lock them in the trunk of a car, etc.
  - Never leave paper or electronic files unattended in a public environment and ensure they are not in open view while in use.
- *Paper records or files*

  To preserve integrity and availability:
  - Take records off-site only when absolutely necessary; whenever practical, the original should remain on-site and only copies removed.
  - Copies should be clearly identified as such and destroyed when no longer needed.
  - Create a sign-in/sign-out procedure with a due-back date to monitor removed files.
  - Whenever possible, remove only relevant documents or an extract or summary.
  - Return records to a secure environment as quickly as possible, for example, at the end of a meeting, the end of the day, or the end of a trip.
  - Ensure that all working copies of paper files containing personal information are returned to the office or a secure environment, and retained according to your institution's records management retention schedule, or disposed of in a secure manner so that the record may not be reassembled and read. Records containing personal or confidential information should never be discarded in a client's or a public trash or recycling bin.
- *Computer and electronic files*

  When using a personal or laptop computer to access electronic files:
  - Ensure the hard drive has only the necessary software programs related to the file.
  - Use an individual's initials, symbols or a code rather than a full name to ensure anonymity of the individual.
  - When communicating with the office, use the highest level of security available. Some examples include double passwords, gateways, data encryption, or remote dial-back system.

- Change passwords on a regular basis (e.g., monthly).
- When more than one person has access to a computer, personal or confidential information should not be retained on hard disk.
- When removing electronic records from the office, copy only the information needed onto a diskette.
- Do not share diskettes or leave them unattended.
- When not in use, store diskettes securely.

• *Physical security*

- Position computer monitors for privacy.
- Never leave a computer unattended with work displayed on the screen.
- Use password protected screen saver options during periods of inactivity.
- Use passwords to protect directories and documents.
- If employees use a network, have the network administrator enable the automatic log-off option.

• *Use of technology*

(telephones, cellular telephones, fax machines, modems, voice mail, e-mail, etc.)

- When making telephone calls from outside the office, safeguard personal and confidential information as much as possible. For example, consider the physical setting to ensure that no one overhears a telephone conversation.
- Never communicate personal or confidential information when using a cellular or cordless telephone. This type of communication can be easily intercepted.
- When the work environment is not conducive to privacy while collecting or communicating personal information, either create a more private environment or collect or communicate the information at another time.

• *Employees Who Regularly Work from Home*

- Designate a secure work area as "office space." For example, employees should work and store files securely in one area.
- If possible, and where appropriate, install a second telephone line dedicated to work-related calls. This is particularly important for employees who need a phone line for a fax or modem.
- Store all paper and electronic records in the most secure fashion available.
- If an answering machine or answering service is required, ensure work-related messages can be accessed only by the employee. It is advisable to have a machine separate from that of the household or to use a password different from the household's to access work-related messages from an answering service.

Educating Employees

Once the policy has been created, institutions should ensure that all employees who telework are aware of the policy and understand it.

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

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

ISSN 1188-7206