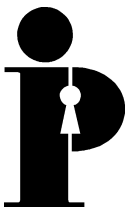
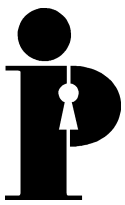
Information
and Privacy
Commissioner/
Ontario

Guidelines for Protecting the Privacy and Confidentiality of Personal Information When Working Outside the Office



Ann Cavoukian, Ph.D.
Commissioner
July 2001



Information and Privacy Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

The Information and Privacy Commissioner/Ontario gratefully acknowledges the work of Colin Bhattacharjee in preparing this report.

This publication is also available on the IPC website.

Table of Contents

1. Introduction

- In the course of performing their duties, provincial and municipal government employees may be required to work outside their employer's conventional office space. This may include transporting records by car, bus, subway, train or airplane; working on assignments or projects at home; attending meetings at hotels and conference centres; appearing at court or tribunal hearings; conducting investigations; making visits to clients or recipients of government services; and representing the government at ceremonies or public gatherings.

- Records containing personal information may be either in paper or electronic format. The purpose of these guidelines is to set out how employees should protect the privacy and confidentiality of such records when working outside the office.

2. Other Sensitive Information

- In certain circumstances, employees who are working outside the office may be dealing with other confidential records that do not necessarily include personal information, such as cabinet submissions, records subject to solicitor-client privilege, or records containing advice to government. Although these guidelines apply to personal information, they are equally applicable to records containing other types of sensitive information.

3. Freedom of Information and Protection of Privacy Legislation

- When working both inside and outside the office, government employees must comply with the *Freedom of Information and Protection of Privacy Act* and/or the *Municipal Freedom of Information and Protection of Privacy Act* (the *Acts*). One purpose of the *Acts* is to protect the privacy of individuals with respect to personal information about themselves held by government.

- Personal information is defined in the *Acts* as recorded information about an identifiable individual, including his or her race, age, family status, address, telephone number, medical or employment history and other information. Both *Acts* contain privacy rules governing the collection, retention, use, disclosure and disposal of personal information held by government. For further details, consult the full text of the *Acts*, which is available on the Information and Privacy Commissioner's Web site at www.ipc.on.ca.

4. Removing Records from the Office

- Employees should only remove records containing personal information from the office when it is absolutely necessary for the purposes of carrying out their job duties. If possible, only copies should be removed, with the originals left in the office.

- Depending on their positions, employees may be required to obtain approval from their manager before removing records containing personal information from the office.

- Records containing personal information that are being removed from the office should be recorded on a sign-out sheet that includes the employee's name, a description of the records; the names of the individuals whose personal information is being removed; and the date the records were removed.

5. Paper Records

- Paper records containing personal information should be securely packaged in folders, carried in a locked briefcase or sealed box, and kept under the constant control of the employee while in transit.

- When an employee travels by car, paper records should always be locked in the trunk. There have been cases, however, where records have been stolen from government employees, including from the locked trunk of a car. Consequently, unless there is no alternative, paper records should never be left unattended in a car trunk while the employee goes elsewhere.

- Paper records should not be opened or reviewed while travelling on public transportation such as a bus, subway, train or airplane.

- When working at home, paper records should be stored in a locked filing cabinet or desk drawer when they are not being used. The cabinet or desk should only contain work-related records.

- When working at other locations outside the office, paper records should be kept under the constant control of the employee, including during meals and other breaks. If this is not possible, the records should be temporarily stored in a secure location, such as a locked room or desk drawer.

6. Electronic Records

- Electronic records containing personal information should be stored and encrypted on a password-protected disk or CD rather than the hard drive of a laptop or home computer.
- To prevent loss or theft, a disk or CD should be carried in a locked briefcase and kept under the constant control of the employee while in transit.
- When working at home, a disk or CD should be stored and locked in a filing cabinet or desk drawer after use.
- When working at other locations outside the office, a disk or CD should be kept under the constant control of the employee, including during meals and other breaks. If this is not possible, they should be temporarily stored in a secure location, such as a locked room or desk drawer.

7. Laptop and Home Computers

- Access to laptop and home computers should be password-controlled, and any data on the hard drive should be encrypted. Other reasonable safeguards, such as anti-virus software and personal firewalls, should also be installed. Employees should only use software that has been approved by their institution's Information Technology department.
- Laptops should be kept under the constant control of the employee while in transit. When an employee travels by car, a laptop should always be locked in the trunk. There have been cases, however, where laptops have been stolen from government employees, including from the locked trunk of a car. Consequently, unless there is no alternative, a laptop should never be left unattended in a car trunk while the employee goes elsewhere.
- If it is necessary to view personal information on a laptop screen when working at locations outside the office, ensure that the screen cannot be seen by anyone else. Personal information should never be viewed on a laptop screen while travelling on public transportation.
- When working at home or at other locations outside the office, a laptop or home computer should be logged off and shut down when not in use. For added protection, they should be locked to a table or other stationary object with a security cable. To the maximum extent possible, the employee should maintain constant control of the laptop, particularly when working at locations outside the office other than home. If this is not possible, it should be temporarily stored in a secure location, such as a locked room or desk drawer.
- Do not share a laptop that is used for work purposes with other individuals, such as family members or friends.

8. Wireless Technology

- Employees should protect the privacy and confidentiality of personal information stored on wireless devices such as personal digital assistants and cell phones. Access to such devices should be password-controlled, and any stored data should be encrypted.

- To prevent loss or theft, a wireless device should be carried in a locked briefcase or closed purse and kept under the constant control of the employee while in transit. Never leave a wireless device unattended in a car. If it is absolutely necessary to view personal information on a wireless device while in public or when travelling on public transportation, ensure that the display panel cannot be seen by anyone else.

- When working at locations outside the office, the employee should maintain constant control of wireless devices. If this is not possible, they should be temporarily stored in a secure location, such as a locked room or desk drawer.

- Do not share wireless devices that are used for work purposes with other individuals, such as family members or friends.

9. Telephones and Voice Mail

- When in transit or working outside the office, employees should avoid using cell phones to discuss personal information. Cell phone conversations can be easily overheard or intercepted by individuals using scanners or other devices.

- If an employee works at home on a regular basis, a separate phone line and password-controlled voice mail box should be set up. Do not disclose the password to family members or roommates.

10. E-mail, Faxes and Photocopies

- When working at home or at other locations outside the office, employees should avoid sending personal information by e-mail or fax. If it is absolutely necessary to do so, follow the practices and tips set out in the Information and Privacy Commissioner's papers on *Privacy Protection Principles for Electronic Mail Systems*, *E-mail Encryption Made Simple*, and *Guidelines on Facsimile Transmission Security*, which are available on the IPC's Web site at www.ipc.on.ca.

- Ideally, employees should undertake the faxing or photocopying of personal information themselves. However, in some locations outside the office, fax and photocopy machines for individual use may not be readily available. If employees must submit records containing personal information to a third party for faxing or photocopying, they should ask to be present when these tasks are being done.

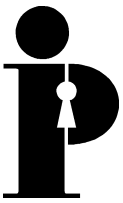
11. Conversations Outside the Office

- Employees should not discuss personal information in public locations such as buses, commuter trains, subways, airplanes, restaurants, or on the street. If it is necessary to do so, move to a location where other persons cannot overhear your conversation.

12. Reporting Requirements

- The loss or theft of personal information should be reported immediately to an employee's immediate manager, the institution's Freedom of Information Co-ordinator, and senior management. If personal information has been lost through theft, the police should be notified as well.

- The loss or theft of personal information should also be reported immediately to the Information and Privacy Commissioner, who may launch a privacy investigation, if necessary. At the outset of an investigation, the IPC may recommend that the institution notify any individuals whose personal information has been lost and take steps to contain the loss of the information.



Information and Privacy Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca