OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for
British Columbia

PROTECTING PERSONAL INFORMATION OUTSIDE THE OFFICE

(Replaces: Guidelines for Protecting Personal Information When Travelling on Business)

February 2005

Whether you're travelling with personal information or working with it at home or another location, personal information can more easily be lost or compromised when it's outside your office. Common sense measures can and should be taken to reduce risks to personal information in such situations.

Private sector organizations covered by the *Personal Information Protection Act* (PIPA) and public bodies covered by the *Freedom of Information and Protection of Privacy Act* (FOIPPA) must take reasonable measures to protect personal information from risks such as unauthorized collection, use or disclosure and are legally liable if they fail to do so. This document offers tips on some steps that can be taken to protect personal information when you take it outside the office and tips on protecting personal information when you're working with it at home.

The following tips apply to "personal information", which is "information about an identifiable individual". The word "organization" is used below to refer to both organizations under PIPA and public bodies under FOIPPA

This document has benefited from a similar publication of the Office of the Information and Privacy Commissioner for Ontario.

Please read the important notice at the end of this document about the nature and status of this document.

WORKING WITH PERSONAL INFORMATION OUTSIDE THE OFFICE

- Never travel with personal information unless you absolutely must have it with you. If you take personal information with you, take the least amount that you need and leave the rest behind. If possible, you should only take copies, leaving original documents in the office.

- While away from your office or your home, laptops and other electronic devices containing personal information (including PDAs such as Palm Pilots and Blackberrys) should be kept with you. If you must leave a laptop or other device somewhere, make sure it is in a location secure from theft, loss and unauthorized access to personal information. (See below for more.)

- Laptops and other electronic devices such as PDAs should be password protected.

- Access to personal information should be password protected, including when stored on a password-protected storage device such as a floppy disk, CD or USB storage drive, rather than the hard drive of your laptop or home computer.

- Electronic records of sensitive personal information when taken away from the office should be encrypted.

- While away from your office or your home, storage devices containing copies of personal information should be kept in a locked briefcase or other container that is kept with you. If you must leave a storage device somewhere, do so in a location secure from theft, loss and unauthorized access to personal information.

- When working outside the office, log off or shut down your laptop or home computer when you're not using it. Set the automatic logoff to run after a short period of idleness.

- When working outside the office, protect your laptop by using locks and alarms as appropriate. As best you can, you should always keep control of your laptop. If this is not possible, you should store your laptop in a secure location such as a locked room or desk drawer.

- Do not share a laptop used for working with private information with other individuals, including family members and friends.

- If the records you need are too voluminous to carry with you, send them to your destination by a trustworthy courier.

- You should avoid viewing personal information in public, including while travelling on airplanes, trains, buses and public transit. Do so only if you absolutely must and take precautions to ensure no one else can view the personal information. For example, your laptop screen should not be viewable by fellow passengers. Set your laptop's screensaver to run after one minute of idleness. Also consider installing a privacy screen filter on your laptop screen, to hinder viewing of the screen from an angle.

- When in transit or working outside the office, avoid using cell phones to discuss personal information. Cell phone conversations can be easily overheard and can be intercepted.

- You should avoid discussing personal information in public, including buses, commuter trains, subways, airplanes, restaurants or on the street. If you must do so, ensure others cannot overhear.

- When travelling or working outside your office you should keep personal information under your control, including during meals and other breaks. If this is not possible, store the personal information in a secure location, such as a locked room or desk drawer. Do not leave personal information in plain view or unattended in an insecure place, such as an unlocked office or meeting room.

- Do not leave records containing personal information in plain view in your hotel room. Consider storing the records at a local office of your organization overnight. If your hotel room or hotel office has a safe, store the personal information there.

- Records containing personal information have gone missing over the years when locked vehicles have been broken into or the vehicle has been stolen. Although the trunk of a vehicle is generally considered more secure than the interior of a vehicle, records have been stolen from locked trunks, so extreme caution must be exercised. Records should only be left in a vehicle if there is no other option. They should be locked in the trunk, not left in plain view in the vehicle interior. They also should be left only if the vehicle is parked in a secure location and then only for brief periods. If a staff person must travel regularly with personal information, a car alarm should be installed to enhance the security of records while in transit.

- When working at home, you should store personal information in a locked filing cabinet or desk drawer when not being used. The filing cabinet or desk should only contain work-related records and no one else should have access to it.

- You should avoid storing personal information on the hard drive of your home computer. Any personal information that is stored on hard drives should be encrypted and password protected. You should ensure your home computer has effective Internet security measures such as anti-virus software and firewalls.

- If you telecommute from home, your employer should provide you with a separate phone line and password-controlled voice-mail box.

- You should avoid sending personal information by email or fax from public locations, including Internet cafes. If it is absolutely necessary to do so, see the tips on email and faxing in other OIPC website resources.

- You should fax or photocopy personal information yourself when working outside the office. If you have to ask someone else to do this for you, you should be present.

- Upon returning to the office, return records to their original storage place as soon as possible or destroy the copies securely. Any working notes you created during the trip that contain personal information should also be stored in a secure environment as soon as possible.

- If personal information is stolen or lost, immediately notify your supervisor and the person responsible for privacy compliance in your organization, file a police report, and notify the OIPC. Your organization or public body should consider notifying the individuals whose personal information has been stolen or lost, telling them the kind of information that has been compromised and steps that are being taken to recover it.

OTHER RESOURCES

Other resources are available to help you meet your obligations regarding working with personal information away from your office, including the following:

- Office of the Information and Privacy Commissioner/Ontario, *Guidelines for Protecting the Privacy and Confidentiality of Personal Information When Working Outside the Office*:
  http://www.ipc.on.ca/images/Resources/wrkout-e.pdf