Office of the
Information &
Privacy Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

Protecting Personal Information Away from the Office

Introduction

Whenever personal information is being used outside of the office there is an increased risk that it will be lost or compromised. Public bodies and private organizations must keep paper and electronic records safe and secure as required by the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Personal Information Protection Act* (PIPA).

Whether you are travelling on a bus or plane, working from home or a remote location, or using portable devices like laptops, USB sticks, and tablets to access personal information outside the office, take the following common sense steps to reduce the risk.

General Rules of Thumb

There are a number of things you can do to protect any personal information you remove from your office:

- Only remove personal information from the office if it is necessary to carry out your job duties.
- Take the least amount of personal information you need and leave the rest behind.
- If possible, take copies and leave the originals in the office.
- Check to see if you need management approval before removing records from the office. Your organization should have a sign-out sheet that includes your name, a description of the records, dates the records were removed and name of the manager who approved their removal.
- Encrypt any electronic device that stores personal information. This includes but is not limited to home computers, USB flash sticks, laptops and mobile phones.
- Avoid viewing personal information collected and used for work in public. If you must, take precautions to make sure no one else can view the personal information.
- Consider installing a privacy screen filter on your laptop screen or monitor when working outside of the office.

- Don't use your personal email as a means to transfer records containing personal information for work purposes. Refer to our USE OF PERSONAL EMAIL ACCOUNTS FOR PUBLIC BUSINESS for more detailed guidance.
- Upon returning to the office, return records to their original storage place as soon as possible or destroy the copies securely.

Working Remotely with Personal Information

If you will be working with personal information from home or remotely, take care to make sure you are the only person able to access the records. Simple steps to take include:

- Log off or shut down your laptop or home computer when you are not using it
- Set the automatic logoff to run after a short period of idleness
- Do not share a laptop used for working with personal information with other individuals, including family members and friends
- When records aren't being used, store in a locked filing cabinet or desk drawer that you have sole access to
- Avoid sending personal information by email or fax from public locations
- If you are using your own device for work purposes, make sure you understand and follow your organizations BYOD (bring your own device) policy

If personal information is stolen or lost, immediately notify your supervisor and the person responsible for privacy compliance in your organization or public body, 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

This document has benefited from a similar publication of the Office of the Information and Privacy Commissioner for Ontario, available at http://www.ipc.on.ca/images/Resources/wrkout-e.pdf

For guidelines on the Use of Personal Email Accounts for Public Business, visit HTTPS://WWW.OIPC.BC.CA/TOOLS-GUIDANCE/GUIDANCE-DOCUMENTS

These guidelines are for information only and do not constitute a decision or finding by the Office of the Information and Privacy Commissioner for British Columbia with respect to any matter within the jurisdiction of the Freedom of Information and Protection of Privacy Act ("FIPPA"). These guidelines do not affect the powers, duties or functions of the Information and Privacy Commissioner regarding any complaint, investigation or other matter under or connected with FIPPA, respecting which the Information and Privacy Commissioner will keep an open mind.