



Introduction to Privacy

What can you expect from this PowerPoint?

- Gain an understanding of privacy
- Learn some key things you can do now to comply with your privacy obligations
- Learn what to do if a privacy breach happens



Core Privacy Principles – Short Description Part 1

- **Accountability:** An organization is responsible for personal information under its control.
- **Identifying Purposes:** An organization should identify the purposes for collecting information at or before the time of collection.
- **Consent:** Where it is appropriate, an individual must have knowledge of and give consent to the collection, use or disclosure of personal information.
- **Limiting Collection:** Personal information should only be collected as necessary for the purposes that the organization has identified.
- **Limiting Use, Disclosure, and Retention:** An organization should not use personal information for new purposes, unless it has the consent of the individual, or as required by law.



Core Privacy Principles – Short Description Part 2

- Accuracy: In order to meet the intended purposes, personal information should be accurate, complete and up-to-date.
- Safeguards: An organization should implement appropriate security safeguards to protect the personal information collected.
- Openness: An organization should be open about its personal information policies and practices.
- Individual Access: Individuals should be informed of the existence, use and disclosure of their personal information.
- Challenging Compliance: Individuals should be able to challenge an organization's compliance with the above principles.

What is the Personal Information Protection Act?

- It is a law in BC.
- It applies to organizations in BC, including non-profit societies.
- It tells you what you need to do to protect privacy.
- It is consent-based, subject to limited exceptions.
- It contains right of access provisions.

Why is it important to protect privacy?



IT'S REQUIRED BY LAW.



IT FOSTERS TRUST AND
ENHANCES CONFIDENCE
IN YOUR OPERATIONS.



IT IS THE RIGHT THING TO
DO.



IT MAKES YOUR JOB
EASIER TO DO.

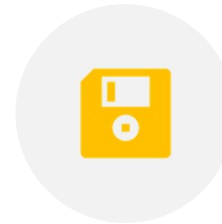
Safeguards – Lock, Hide, Shred



**LOCK YOUR FILING
CABINETS.**



**HIDE YOUR FILES FROM
VIEW.**



**DESTROY FILES
CONFIDENTIALLY.**



**DON'T LEAVE FILES
AND LAPTOPS
UNATTENDED IN CARS.**

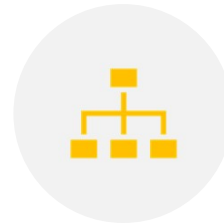
Safeguards – Be Confidential



TAKE STEPS TO PREVENT OTHER
TENANTS OR EMPLOYEES FROM
SEEING OR HEARING
CONFIDENTIAL INFORMATION.



ACCESS FILES ONLY WHEN IT'S
NECESSARY TO DO YOUR JOB.



SHARE INFORMATION ONLY IN
ACCORDANCE WITH YOUR
ORGANIZATION'S POLICIES.



VERIFY IDENTIFY BEFORE YOU
SHARE INFORMATION.

Safeguards – Be Technology Savvy



USE A STRONG PASSWORD AND DO NOT SHARE IT.



DON'T STORE PERSONAL INFORMATION ON PORTABLE DEVICES. IF YOU HAVE TO, MAKE SURE THE DEVICES ARE ENCRYPTED.



EMAIL IS LIKE A POSTCARD. USE EMAIL WISELY.

Privacy Breaches

–

What do you do when a privacy breach happens?

- Report immediately to the person in your organization who is responsible for privacy
- Contain the breach (recover the information, stop it from being spread any further)
- Remediate by investigating what happened, resolve the incident, and notify affected individuals
- Prevent it happening again, e.g. training, change to a process

Requests from individuals for access to their records

- Individuals have a right of access to their files under PIPA
- Make reasonable effort to assist the applicant.
- Respond within 30 days, unless PIPA section 31 permits you to extend.
- Give the applicant the reasons for any redactions.
- Give the applicant the name of a person who can answer questions about the refusal.
- Advise the applicant that they can ask for a review of your decision.

Requests from Individuals for access to their records

- What can/must you redact?
- Can redact:
 - information protected by solicitor client privilege.
 - information of a confidential, proprietary nature.
- See PIPA section 23 for all the information you can or must redact.

Requests from Law Enforcement

- How should you deal with requests from law enforcement agencies?
- Follow your organization's policy.
- Make sure the caller is who they say they are. You can do this by getting their name and number, verifying the number and calling them back.
- Make sure they are conducting an investigation. You can do this by asking for a police investigation number.
- Give only the information you are being asked for.
- Document your actions.

Requests from other third parties

- How should you deal with requests from third parties?
- Follow your organization's policy.
- Make sure the caller is who they say they are.
- Make sure you have the authority to disclose. Just because an official organization is asking, it doesn't mean you can and should give them the information.
- Give only the information you are being asked for.
- Document your actions.

Resources

- OIPC Investigation Report:
<https://www.oipc.bc.ca/investigation-reports/2141>
- OIPC Securing Personal Information: A Self-Assessment Tool for Organizations
<https://www.oipc.bc.ca/guidance-documents/1439>
- OIPC Privacy Breaches: Tools and Resources
<https://www.oipc.bc.ca/guidance-documents/1428>
- BC Housing Privacy Toolkit:
<https://www.bchousing.org/partner-services/non-profit-training-resources/privacy-toolkit>