



Privacy and Access in British Columbia

B.C.'s Freedom of Information and Protection of Privacy Act

Jeannette Van Den Bulk

Manager, Legislation and Strategic Privacy Initiatives

Knowledge and Information Services Branch

Ministry of Labour, Citizens' Services and Open Government

March 28, 2011



Today's Agenda

Introductions

This Session:

- A high level overview of the *Freedom of Information and Protection of Privacy Act* (FOIPPA Act) including:
 - Introduction to the FOIPPA Act
 - Privacy – collection, use, disclosure, security and retention of personal information
 - Access – “FOI” rights, process, exceptions (including Public Interest Paramount & Emergency Disclosure)
 - Privacy & Security
 - Information Incidences (including Privacy Breaches)
 - Privacy Tools

Knowledge and Information Services Branch

- **Information Services**

- Governance with regard to: privacy, legislation, information sharing, access
- Responsible for the *Freedom of Information and Protection of Privacy Act* (FOIPPA Act), *Personal Information Protection Act* (PIPA), *Document Disposal Act* (DDA), and *Electronic Transactions Act* (ETA) and all policy, standards and directives that flow from them.
- Leadership, support and services to government and other public bodies to assist them in complying with their privacy and access obligations.

- **Knowledge Services**

- Office of the Government Chief Information Officer (OCIO) Policy
- Research Services provided across government
- Evaluation Support
- Accompanying education and training

Information and Privacy Commissioner

- Information and Privacy Commissioner is an independent Officer of the Legislature
- Elizabeth Denham is B.C.'s Information and Privacy Commissioner
- The Office of the Information and Privacy Commissioner (OIPC):
 - conducts reviews and investigations to ensure compliance with the FOIPP Act
 - mediates FOI disputes
 - comments on FOI and privacy implications of proposed legislative schemes or public body programs



FOIPP Act is distinct from B.C. private sector and federal legislation

Freedom of Information and Protection of Privacy Act (FOIPP Act)
public sector access and privacy legislation; applies to “public bodies” in B.C.

Personal Information Protection Act (PIPA)
private sector privacy legislation; applies to “organizations” (more than just businesses) in B.C.

Personal Information Protection and Electronic Documents Act (PIPEDA)
applies to federal works, undertakings or businesses (banks, airlines, and telecommunications companies) applies to the collection, use and disclosure of personal information in the course of a commercial activity and across borders.

Canada’s ***Access to Information Act*** and also the ***Privacy Act***
are the federal equivalents to the BC FOIPP Act (access and privacy obligations for federal government institutions and the federally regulated)



Structure of the Act - Overview

- Part 1: Introductory Provisions
- Part 2: Freedom of Information
- Part 3: Protection of Privacy
- Part 4: Office and Powers of Information and Privacy Commissioner
- Part 5: Reviews and Complaints
- Part 6: General Provisions
- Schedule 1: Definitions
- Schedules 2 and 3: List public bodies



Purposes of the FOIPP Act (s. 2)

“make public bodies more accountable to the public and to protect personal privacy by”

1. giving the public a right of access to records
2. giving individuals a right of access to, and a right to request correction of, personal information about themselves
3. specifying limited exceptions to the rights of access
4. preventing the unauthorized collection, use or disclosure of personal information by public bodies, and
5. providing for an independent review of decisions made under this Act.



Coverage of the FOIPP Act

APPLIES TO:

all **records**
in the **custody** or under the **control**
of a **public body**

There are numerous B.C. **public bodies** covered including government ministries, colleges, universities, school boards, hospitals, health boards, governing bodies of professions, municipalities, regional districts and police boards.

Coverage of the FOIPP Act

Section 3(1)(e) – This Act ...does not apply to...

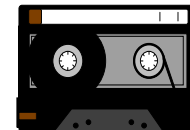
...a record containing teaching materials or research information of employees of a post secondary education body...

Teaching Materials - Notes prepared by a university professor to refer to while presenting a lecture to students.

Research information - A bibliography prepared by a research assistant at a university to enable a professor to determine what background material is relevant to a research proposal.

What is a “Record”?

- A “record” is any information recorded or stored by any means whether in hard copy or in electronic format
- This includes books, documents, maps, drawings, photographs, letters, e-mails, telephone records, black books, vouchers, papers, etc...





What Does “Custody” Mean?

- Physical possession of the record
- May not be responsible for the actual content of the record
- Responsible for providing access to and security of the record
- Responsible for managing, maintaining, preserving and disposing of the record

What Does “Control” Mean?

- Control means:
 - Authority to manage, restrict, regulate or administer the use or disclosure of a record
- Indicators of control are that the record:
 - was created by an employee of a public body,
 - was created by a consultant for the public body,
 - is specified in a contract,
 - is subject to inspection, review or copying by the public body under contract.



What if the Public Body Doesn't Have Custody?

Example

- School hires a private consultant to prepare a report to analyze student use of campus vending machines
- School implements changes based on the report
- General request is received under the FOIPP Act for a copy of the report but a copy cannot be found in the school files
- Can the school argue it doesn't have a copy of the record, only the consultant has custody (and the consultant is not covered by the FOIPP Act)?

Protection of Privacy

To protect personal privacy by preventing the unauthorized collection, use, or disclosure of personal information by public bodies.





What is privacy?

- It is not defined in the *Freedom of Information and Protection of Privacy Act* (FOIPPA), the *Personal Information Protection Act* (PIPA), or any legislation in Canada
- None of the statutes define “privacy” but aim to achieve it with rules for how personal information is to be collected, used and disclosed.
- Different types of privacy:
 - physical, spatial, informational

The foundation of privacy laws

- Informational self determination
 - an individual's personal information is their own
 - to the extent possible, the individual controls how their personal information is collected, used and disclosed
- This is reflected in a Code of Fair Information Practices...

FAIR INFORMATION PRACTICES





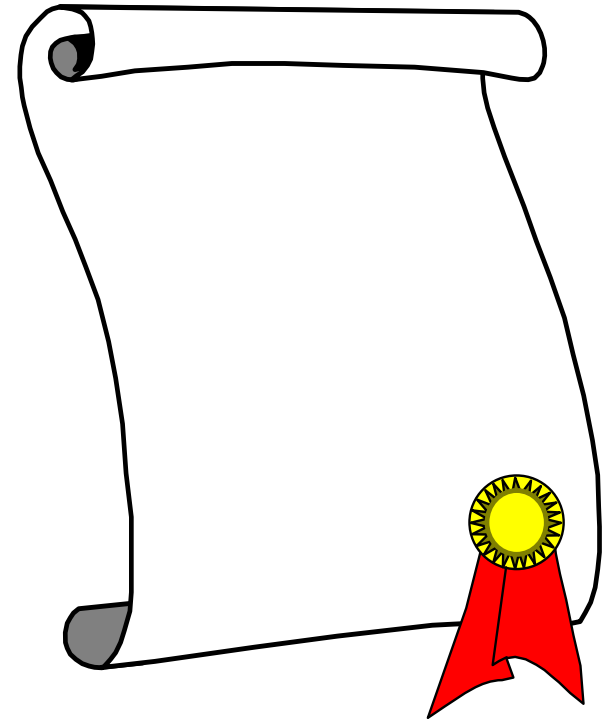
Code of Fair Information Practices

Places limits on:

- collection, use and disclosure of personal information (s. 26, 27, 32, 33, 33.1 and 33.2)

Requires:

- accuracy and completeness (s. 28)
- access (Part 2) and correction (s.29)
- reasonable security (s. 30)
- retention of records (s.31)





What is “Personal Information”?

“Personal information” means recorded information about an identifiable individual other than contact information”

(Schedule 1 definition in the FOIPP Act)

Examples of your personal information:

- Your race, national/ethnic origin, skin colour
- Your religious or political beliefs or associations
- Your age, sex, sexual orientation, marital status
- Your fingerprints, blood type, DNA information, biometrics
- Your health care, educational, financial, criminal, employment history
- Your opinion unless it is your opinion about someone else



Collection of Personal Information (s.26)

- Key to protecting privacy
- Personal information can only be collected if:
 - Authorized under an Act
 - For law enforcement
 - Related directly to and necessary for an operating program or activity
- Consent is not an authority for collection

How Personal Information is Collected (s.27)

- Information must be collected directly from the individual, except in limited circumstances.
- Must notify the individual of the purpose, the legal authority, and who to contact with questions, except in limited circumstances.



Collection of Personal Information (s.26)

Example

Public body wants to collect personal information which might be handy in the future. It ensures it only collects information from those who have signed informed consents



Collection of Personal Information (s.26)

Example

Faculty staff feel a new course in a specialized subject area would be beneficial to the overall program.

Before they begin the work of creating the course, they want to canvas program students to ensure there would be sufficient interest; they would also like to run a draft of a proposed course outline by the students for feedback. It would also require finding out some academic information either directly from the student or from student files to ensure the students' comments are relevant to any decisions that may result.

Are they authorized to collect this information?



Use of Personal Information (s.32)

A public body may only use personal information:

- For the purpose for which it was obtained or compiled, or for a consistent purpose.
 - A consistent purpose (s.34):
 - has a reasonable connection to the original purpose, and
 - Is necessary to perform the duties of, or for operating a legally authorized program, of the public body
- If the individual has consented to the use.
- For a purpose for which the personal information has been disclosed to it under the Act.



Use of Personal Information (s. 32)

Example

Public body has already collected employee home addresses for tax purposes and now wants to use the information to send employees birthday cards.

OR

Public body wants to use student email addresses to canvas students for suggestions to improve registration services.



Use of Personal Information (s.32)

Example

The Physical Education Department has already collected photographs from a campus sporting event. Administration now wants to use the photographs to promote the school on its website.

Is this an authorized use of personal information?



Disclosure of Personal Information (ss. 33, 33.1, 33.2)

Disclosure only in limited circumstances

For example:

- Consent (written)
- For the purpose for which was obtained or compiled or a consistent purpose
- If an enactment authorizes disclosure
- To comply with a subpoena, warrant, or order

Inside versus outside Canada

Disclose based on a need to know

- limit distribution
- limit content



Disclosure of Personal Information (ss. 33, 33.1, 33.2)

Example

- A student, who is the subject of a number of investigations regarding violations of academic integrity, has behaved aggressively in the past in dealing with faculty staff.
- The investigation file has been annotated with a warning about this behaviour.
- Can this information be shared with staff members in other departments so that they can take precautions when dealing with the individual?



Disclosure of Personal Information (ss. 33, 33.1, 33.2)

Example

An individual calls your office claiming that he is a police officer and wants to know the home address of one of your employees?

What do you do?



Disclosure for Research Purposes (s. 35)



Disclosure for Archival or Historical Purposes (s. 36)



Accuracy & Completeness (s. 28)

Public body must make every reasonable effort to ensure that personal information is accurate and complete when used to make a decision

The Right to Correction (s. 29)

Individual has right to request correction of personal information

- Assume what you write will be viewed by the individual
- Ensure language is clear and understandable; avoid jargon and labels – be objective
- s.29 applies to factual errors or omissions in personal information, not to expressions of judgement
- s.29 does not function as an avenue for appeal

Retention (s. 31)

- Must retain personal information for at least 1 year if used to make a decision that directly affects the individual; for reasonable opportunity for access;
- Ensure any other applicable legal and policy requirements met



Access to Information a.k.a. Freedom of Information (FOI)



Overarching Purpose

“the overarching purpose of access to information legislation, then, is to facilitate democracy. It does so in two related ways. It helps to ensure first, that citizens have the information required to participate meaningfully in the democratic process, and secondly, that politicians and bureaucrats remain accountable to the citizenry.”

Justice Laforest, in a landmark Supreme Court of Canada decision in *Dagg vs. Canada*



A Culture of Openness

- Increased transparency
- Alters how public bodies handle information
- Common sense (What if it were my information?)
- Not to replace other existing methods of access (except for personal information)
- Avenue of last resort





Right of Access

The public has a right to request access to any record in the custody or control of a public body (s.4)

➤ Includes the right to seek access to personal information whether in a case file, or elsewhere (e.g. email and memos)

BUT right of access limited by exceptions to disclosure (s.12 – 22.1)

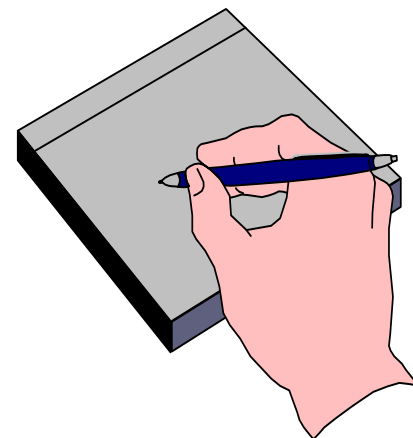
AND subject to payment of fees as required (s.75)

Note: no fees if the request is for the applicant's own personal information

The Request Process (s.5)

The applicant:

- Must make a written request
- Must provide sufficient detail to identify record sought
- May ask for a copy or to examine record
- Must provide proof of authority if acting for another person*
 - persons under 19 years of age
 - persons who have committees
 - deceased persons



* See also s. 3 of the FOIPP Act Regulation



What is Needed for an FOI Request?

Example

Applicant handwrites a letter to the public body, providing their name and address, and stating the following:

“Give me a copy of John Smith’s Report dated June 1, 2007”

Applicant fails to use the school FOI request form or even cite the FOIPP Act?

What are the public body’s obligations?



Request Considerations

- **Duty to assist (s.6)**
- **Does a record exist?**
- **Does public body have custody or control?**
- **Time Limit (s.7) & Time Extensions (s.10)**
- **Transfer? (s.11)**
- **Do 3rd parties need to be notified?**
- **Fees & Exceptions**



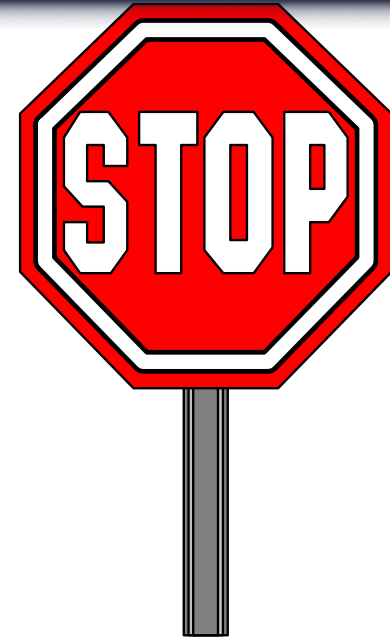
Exceptions and Severing: Applying Exceptions to Disclosure

- Must release unless an exception applies
- Disclosure should be the rule, not the exception
- Two types of exceptions:

Mandatory and Discretionary

Mandatory Exceptions

The head must not release requested information:



- Section 12: Cabinet confidences
- Section 21: Third party business information
- Section 22: Disclosure harmful to personal privacy
- Section 22.1: Related to abortion services



Discretionary Exceptions

The head of a public body may refuse to disclose requested information

Two parts to applying a discretionary exception:

- Does the exception apply?
- Exercise discretion



Discretionary Exceptions

Include:

- local public body confidences (section 12)
- policy advice or recommendations (section 13)
- legal advice (section 14)
- law enforcement (section 15)
- disclosure harmful to intergovernmental relations (section 16)
- disclosure harmful to financial or economic interests of the public body (section 17)
- disclosure harmful to conservation of heritage sites (section 18)
- disclosure harmful to individual or public safety (section 19)
- information to be released in 60 days (section 20)



Exercising Discretion

- The purpose of the Legislation
- Balance of interests (what is purpose of exception)
- Severing
- Historical practice
- Nature of the record
- Will disclosure increase public confidence?
- Age of the record
- Sympathetic or compelling need
- Previous orders



Public Interest Paramount – s. 25

Overrides any other provision of the Act:

- Whether or not request for access made
- Must release *information*, without delay
- To the public, affected group or applicant
- Information about a risk of significant harm to environment or health or safety of the public or a group of people; or other disclosure which is, for any other reason, clearly in the public interest.

s.25 Public Interest Paramount –

Information must be disclosed if in the public interest

Example – *significant risk of harm to the public*

- Counsellor observes angry student expresses deep despair & hopelessness;
- Student blames others for their misfortunes, expresses ideas of “getting even” and has no known friends;
- Counsellor reads student’s essays that are violent, graphic and disturbing;
- Counsellor reads student’s blog posts that are also disturbing, self-aggrandizing and even with a picture depicting the student with what looked like an improvised explosives device;
- Counsellor’s professional opinion is the student is on the verge of a breakdown and is concerned student will harm self or others;
- Counsellor recognizes the duty to respect the student’s privacy but believes there is a significant risk.

Is the Counsellor authorized to disclose the student’s personal information?



Emergency Disclosure – *other relevant sections of the FOIPP Act*

s. 33.1(1)(m) – if head determines compelling circumstances affecting anyone's health or safety – Note: notification is required unless harm to someone's health or safety

s. 33.1(1)(n) – so that the next of kin or a friend of an injured, ill or deceased individual may be contacted

s. 73 – no action lies and no proceeding may be brought against... a public body, the head... or any person acting on behalf of or under direction of the head of a public body for damages resulting from... disclosure... in good faith...

s. 79 – if conflict with provision(s) of other Act(s) – FOIPP Act prevails unless explicitly overridden



Disclosure of Personal Health Information

Example – *significant risk of serious bodily harm*

- Student is receiving psychological treatment at the college's counselling centre;
- Student's psychologist has noted severe depression in student and suspects abuse of prescription drugs;
- Psychologist believes there may be a risk of suicide and would like to involve student's family physician, immediate family member or emergency contact;
- Student specifically instructed psychologist *not* to disclose their personal health information to anyone;
- Over week-long reading break, student calls psychologist from out of town with slurred speech and threatening to end their life.

What can the psychologist do?



Emergency Disclosure – resources

“Practice Tool for Exercising Discretion: Emergency Disclosure of Personal Information by Universities, Colleges and other Educational Institutions”

October 2008 – OIPC for BC & the Information and Privacy Commissioner of Ontario

- Have clear policy & procedure for emergency situations;
- Regularly educate & train staff on the policy & procedure and the basics of what privacy law permits in emergency situations;
- Provide notice to students about the possibility of emergency disclosure of personal information without consent;
- Notification of a threat or an emergency alert should be readily available to all members of a college or university community;
- Ensure clear decision-making roles & responsibilities with a pre-established communication method;
- Educate, Train, Practice, Evaluate

Privacy and Security



Management of Personal Information

- Ensure you have authorities for collection, use and disclosure of personal information before you implement an initiative, and consider the potential consequences to privacy
- Limit use to original purpose or *consistent purpose* (beware of “scope creep”/ “function creep”)
- Set strict policies for security, retention and destruction of personal information from the outset, not as an afterthought
- Limit disclosure and data-sharing to need-to-know principle





FOIPP Act: security measures

- A public body must make reasonable security arrangements to protect personal information (s.30)
- Should be appropriate and proportional to the sensitivity of the personal information e.g. suspension information vs lunch order
- Storage & Access must be in Canada (s.30.1)
- Safeguards should include:
 - Physical measures (e.g. locked file cabinets, restricted access to offices)
 - Technological measures (e.g. user IDs, passwords, encryption)
 - Have policies and procedures for keeping files secured



Security Tips

- Security is only as good as its weakest link (train staff, conduct periodic reviews)
- Consider internal security ‘threats’ – including those from privacy-unaware staff (limit access to “need to know”; consider audit trails)
- Protect personal information throughout its lifecycle (e.g. “clean desk” policy for current records; properly storing inactive records; properly disposing of records and equipment)



Information Incidences

Information Incidences are ALL unauthorized event(s) that threaten the privacy or security of information

Includes privacy breaches: a collection, use, disclosure, disposal, storage of or access to personal information, whether *accidental or deliberate*, that is not authorized by the *Freedom of Information and Protection of Privacy Act*



Examples of How Information Incidences occur

- *Employee errors such as mis-stuffed envelopes or incorrect email addresses*
- *Hacking or phishing*
- *Sale of unwiped hardware or blackberries*
- *Wrong fax numbers or addresses*
- *Deliberate employee misconduct*



PRIVACY BREACH RESPONSE

A privacy breach can affect any organization, even if it has good privacy and security practices. Are you ready for a privacy breach and do you know what to do when one occurs?

New Government of British Columbia Information Incident Management Process

Step 1 - Report

Ministries must follow. All public bodies should create their own policy and process.

Step 2 - Recover

See the Office of the Government Chief Information Officer website for information:

<http://www.cio.gov.bc.ca>

Step 3 - Remediate

OIPC Breach Resources for Public Bodies at:

<http://www.oipc.bc.ca>

Step 4 - Prevent



It's better to prevent a privacy breach in the first place!

Prevent breaches through compliance with the general FOIPP Act requirements, for example:

- Awareness of the disclosure authorities and other provisions of the FOIPP Act
- Reasonable policy and procedures for disposition of personal information (not selling old hard-drives; etc)
- Reasonable security arrangements, including physical, technical and policy measures (encryption; establishing sound access user profiles; etc)

Protect personal information throughout its lifecycle
(e.g. storing inactive records, destroying records –
certificate of destruction)

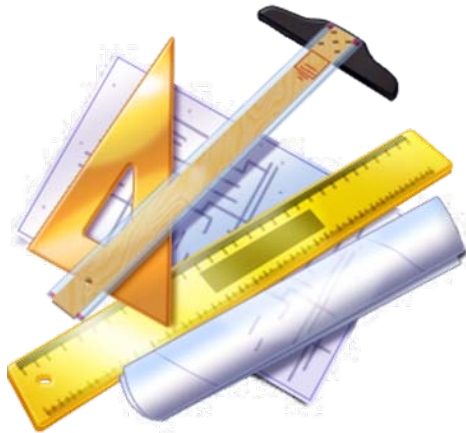


Is this enough?

Organizations and public bodies need to think about:

- Whether mechanisms are in place to prevent unauthorized disclosure
- Whether employees are made aware of and understand policies and procedures (even employees working at the lowest level)
- The sufficiency of monitoring, training and supervision given to staff
- The use of proper equipment, systems and technology that is updated and well maintained
- Whether employees have access to managers or other experts when questions arise
- Whether an emergency plan is in place to deal with unintentional disclosure (do employees know who to report problems to?)

Privacy Tools





Privacy and the administration of personal information

- Organizations and public bodies have millions of pieces of personal information, on paper, in databases, on laptops, etc.
- What tools are available to keep track of this information and ensure it is administered appropriately?



Privacy Impact Assessment: When should one be done?

- New program, project, system, legislation, technology, or other initiative; OR
- If there are significant changes to them (a PIA is a living document); OR
- Any time personal information will be collected, used or disclosed (shared)



Privacy Impact Assessment: Benefits

- If used as part of normal business processes, the PIA can ensure that privacy requirements are identified and satisfied in a timely and cost efficient manner.
- PIA process is also designed as an educational tool – participating in privacy impact assessments promotes privacy awareness.
- The PIA can make the difference between a privacy invasive and a privacy enhancing initiative, without compromising business objectives or adding significant costs.

Information Sharing Agreements (ISA)

What is an ISA?

- When should an ISA be used?
- Components of an ISA
- What are the benefits of an ISA?



ISA Best Practices / Guidelines:

http://www.cio.gov.bc.ca/local/cio/priv_leg/documents/foippa/guidelines_isa.pdf

Information Sharing Agreements (ISA)



Example

- Public body feels it has FOIPP Act authority to, and wants to, share personal information with another public body
- But, the public body wants assurances the other public body will protect the personal information as it should
- It wants to know if any privacy breaches occur so the public body can appropriately respond if necessary



Privacy Protection Schedule

Mandatory for ministries; recommended for other public bodies and organizations.

Advice for other public bodies

The PPS for use by other public bodies may be completed and attached as a schedule to any contract between a public body and a contractor under which the contractor will be collecting, creating, using, disclosing or storing "personal information" (as defined in the FOIPP Act) unless it is not intended that the public body will own or control the personal information.



Contractor Obligations: Privacy Protection Schedule

Example:

School brings in a contractor to set up a database and keep track of all student grades and disciplinary matters on behalf of the school.

The contractor stores its database on servers in the USA.

Has the school met its FOIPP Act responsibilities?



Useful Links

Knowledge and Information Services Branch:

<http://www.cio.gov.bc.ca/cio/kis/index.page?>

OCIO – Freedom of Information and Protection of Privacy - Public Sector (includes Policy & Procedures Manual; PIA Process with Template; Contracting link to PPS; etc): http://www.cio.gov.bc.ca/cio/priv_leg/foippa/index.page?

The Freedom of Information and Protection of Privacy Act:

http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/96165_00

BC Office of the Information and Privacy Commissioner: <http://www.oipc.bc.ca/>

Federal – Office of the Privacy Commissioner of Canada: <http://www.priv.gc.ca>

Useful Resources

FOIPPA Policy and Procedures Manual

http://www.cio.gov.bc.ca/cio/priv_leg/manual/index.page?

- Emergency Disclosure of personal information by Universities, Colleges and other institutions
- Key Steps to Responding to Privacy Breaches
- Protecting Personal Information Outside the Office
http://www.oipc.bc.ca/index.php?option=com_content&view=article&id=55&Itemid=76



Contact Information

BC Privacy Helpline: 250-356-1851

(Enquiry BC 1 800 663-7867)

CPIAADMIN@gov.bc.ca



Questions?



BRITISH
COLUMBIA
The Best Place on Earth



BRITISH
COLUMBIA

The Best Place on Earth