COMMUNITY LIVING
BRITISH COLUMBIA

Policy Number:	Policy Section:	Effective: February 22, 2012
QA7.102	Quality Assurance	**Amended:** August 8, 2012 **Amended:** May 1, 2015
Title:	**Executive Sponsor:**	
Protection of Information Policy	Director, Quality Assurance	

1. PURPOSE

This policy describes CLBC staff responsibilities for protecting sensitive and personal information in CLBC's custody. It also describes specific required practices for staff when they are working in the office as well as working outside the office, to preserve confidentiality and prevent information incidents and privacy breaches.

This policy is one of a suite of privacy related policies listed in the *Organizational Privacy Policy*. These policies are supplemented by the *CLBC Privacy Guidelines* which provide an overview of privacy legislation and best practices.

2. DEFINITIONS

Information Incident: A single or a series of unwanted or unexpected events that threaten privacy or information security. Information incidents include the unauthorised collection, use, disclosure, access, disposal, or storage of personal or sensitive information, whether accidental or deliberate.

Personal Information: Information recorded about an identifiable individual, including, but not limited to:

- name, address, telephone number, email
- race, national/ethnic origin, colour, religious or political beliefs or associations
- age, sex, sexual orientation, marital status
- identifying number or symbol such as social insurance number or driver's license number
- fingerprints, blood type, DNA prints
- health care history
- educational, financial, criminal, employment history
- anyone else's views or opinions about an individual and the individual's personal views or opinions unless they are about someone else

Personal information also includes separate pieces of information that may seem unrelated, but when put together would allow someone to accurately infer information about an individual.

Privacy Breach: Information incidents are called privacy breaches when they involve collection, use, disclosure, access, disposal, or storage of **personal** information, whether accidental or deliberate, that is not authorized by the *Freedom of Information and Protection of Privacy Act*.

Privacy Officer (PO): A designated position within CLBC with overall responsibility and accountability for CLBC privacy policies and related compliance with the *Freedom of Information and Protection of Privacy Act*. The Director, Quality Assurance is CLBC's Privacy Officer.

Sensitive Information: Information or data that is confidential or critical to the functioning of CLBC, or which CLBC is obliged under law or by government to maintain and keep confidential, and any other information or data that could harm CLBC or individuals, if compromised.

3. POLICY

CLBC maintains information security, including security of personal information, through safe information management practices. These practices include maintaining a "clean desk" at work, keeping sensitive or personal information secure when working outside of the office by using appropriate security measures with mobile computing devices, portable storage devices, cellular phones, as well as when using remote access privileges, handling physical documents and keeping premises secure.

CLBC requires staff to secure personal information in order to protect it from unauthorized access, collection, use, disclosure, copying, modification or disposal. Physical safeguards include the use of locked filing cabinets, limiting material on desks, counters, meeting room tables, proper use of fax machines and copiers, and physically securing locations where personal information is held for employees who handle personal information. Electronic safeguards include the use of passwords, encryption, firewalls and other information security practices such as those described in the CLBC *Organizational Information Security Policy,* the CLBC *Internet and Technology Agreement* and CLBC *Organizational Privacy Policy*.

All CLBC employees who work with personal or sensitive information outside the workplace must have prior approval to work with this type of information off site and are personally responsible for protection of the information while off site, as outlined in the *Freedom of Information and Protection of Privacy Act* and CLBC's *Privacy Guidelines.*

4. PROCEDURES

4.1 General:

All staff must comply with the following general expectations to maintain information security:

- Protect sensitive and personal information from misuse, disclosure and tampering.
- Exercise due care in handling sensitive and personal information.
- Do not reveal your IDIR/password combination and PARIS or other systems password and User ID combinations. These should be known only to you.
- You are accountable for all actions performed with your IDIR and password.

- Do not use the same passwords for personal computing. It is good practice to use different passwords for various accounts so anyone obtaining one password will not have access to all your accounts.
- Use assigned equipment safely by following the instructions of management, information management or information security personnel.
- Increase telephone and other communications security by conducting business calls in a private area to reduce the likelihood of being overheard, confirming participants on conference calls before commencing discussion, identifying callers before releasing information.
- Adhere to the requirements of this policy and the *Protection of Information Policy Checklist* as well as the *Use of Email and Fax Policy,* the *Use of Social Media Policy,* the *Mobile Device User Policy* and the CLBC *Internet and Technology Agreement*.
- Do not intentionally subvert, bypass or corrupt security measures such as firewalls or antivirus programs.
- Report any actual or suspected loss, theft or misuse of information or devices.

4.2 At the office:

Staff must ensure that their assigned desk and office space is maintained as set out below:

- When an individual, representative or family member is at the desk, ensure only that individual's paperwork is on the desk.
- Store sensitive or personal information securely before leaving the desk for any reason. Do not leave sensitive or personal information documents on the desk over night or take printed copies home.
- Photocopy sensitive or personal information only if it is required and ensure copies are not left on the copier.
- Ensure computing devices have default printers set to the correct printers for the office.
- Do not store sensitive or personal information documents on their local drive, download or use unauthorised software, leave printed documents unattended, dispose of sensitive or personal information in recycle bins or leave written passwords easily accessible to unauthorized persons.
- Be observant of unauthorised persons visiting the office or looking through windows.
- At the end of the working day, lock up or shred copies of sensitive or personal information paperwork (as appropriate), empty the shredder basket, ensure access points such as windows and doors are locked and secure and lock laptops overnight.

4.3 When working from home or outside their assigned work space:

Staff must adhere to the following security measures:

- Use CLBC approved equipment for mobile computing.
- Never leave any equipment unattended in public.
- Do not access sensitive or personal information over unsecured public computers or public wireless networks, for example hotspots at airports or coffee shops.
- Lock equipment in the trunk of your car when in transit.

- Use remote network access services such as Desktop Terminal Service (DTS), Virtual Private Network (VPN) and/or Citrix when connected via a wireless network only if you are authorized by your manager.
- Do not download, save, store or print sensitive or personal information on private computers or devices.
- Protect mobile computing devices, such as laptops and smart phones, by locking them up when not in use and by using password protection and other security measures as directed.
- Take extra care with portable storage devices and smart phones, including ensuring password protection is on and keeping the device on your person.
- Do not download, save or store sensitive or personal information on mobile devices.
- Do not bypass or disable the security protections and controls set on issued mobile devices.
- Do not allow unauthorized access to issued equipment or remote access accounts, including by family members.
- Ensure that current antivirus and anti-malware software is installed on any non-CLBC computing device used.
- Keep control of and safeguard work materials at all times.
- Do not take paper or physical records out of the office unless necessary for specific tasks.
- Keep all records containing personal or sensitive information with you when out of the office.
- Lock any paper or physical records taken out of the office in the trunk of the car while you are driving.
- Do not leave any records in a vehicle or other non-work location when you are not present.
- Return paper or physical records to the office secure filing room as soon as possible.

4.4 Managers are responsible to:

- Ensure that the expectations of this policy are met by employees and promptly address any discrepancies.
- Ensure staff are aware of and comply with information security practices to protect sensitive and personal information under their care and control.
- Provide approval as appropriate for individual staff to work outside the office with personal or sensitive information.
- Report all information incidents and privacy breaches to the Director, Quality Assurance and address as required by the Director, Quality Assurance.
- Authorize staff access to CLBC information systems only as needed for their role.
- Address risks prior to granting remote access privileges to contractors including ensuring contractors' devices are scanned for vulnerabilities prior to connecting to the government network.
- Maintain good document management and filing practices to ensure documents containing sensitive or personal information are secure and made available only to the appropriate staff.
- Arrange for appropriate visitor sign in and out procedures in the office.
- Develop and communicate procedures for when an unauthorised person is found on the premises.

4.5 The Privacy Officer is responsible to:

- Consult with managers regarding issues related to the security of sensitive or personal information.
- Work with Director, Information Technology on matters of technology and information security interface and procedures for managing information incidents and privacy breaches.
- Monitor the development and implementation of CLBC privacy protection and information security measures to ensure they meet legislative and policy requirements.

4.5 The Director, Information Technology is responsible to:

- Develop and maintain up to date information security practices and procedures.
- Develop and maintain provisioning procedures for staff and contractors which allow access to personal information only on a need to know basis.
- Work with the Privacy Officer to promote, evaluate and update procedures to protect and maintain personal information.

5. DOCUMENTATION

5.1 Document all information incidents and privacy breaches as advised by the Director, Quality Assurance.

5.2 Maintain records of equipment assignments and recovery, visitor records, and other relevant information security controls.

6. PRACTICE

6.1 Staff should keep information security practices in their mind at all times, including when making phone calls, receiving or sending emails or faxes, using computing devices, mobile phones, working at their desk, etc.

6.2 Staff action is key to protecting information. Staff awareness of information security issues is essential for good information security practices.

7. REFERENCES

Confidentiality and Information Sharing Policy
Internet and Technology Agreement
Mobile Device User Policy
Organizational Information Security Policy
Organizational Privacy Policy
Protection of Information Policy Checklist
Use of Email and Fax Policy
Use of Social Media Policy
Freedom of Information and Protection of Privacy Act