



Policy Number: QA7.061	Policy Section: Quality Assurance	Effective: March 2, 2011 Amended: November 24, 2016
Title: Organizational Privacy Policy		Executive Sponsor: Director, Quality Assurance

1. PURPOSE

This policy describes CLBC’s approach to privacy of personal information. It provides general direction for all staff working with the personal information of individuals served by CLBC or of CLBC employees. It is rooted in and exceeds the requirements of the BC *Freedom of Information and Protection of Privacy Act* (FOIPPA). The *Organizational Privacy Policy* is an overarching policy which complements the *CLBC Privacy Guidelines* and is complemented by a suite of more detailed policies dealing with specific aspects of privacy and confidentiality.

2. DEFINITIONS

Confidentiality: The obligation to keep others’ personal information private, secret and safe from access, use or disclosure by people who are not authorized to have that personal information.

Consistent Purposes: Use and disclosure of personal information is considered consistent if the use and disclosure has a reasonable and direct connection to the purpose for which it was originally collected and is necessary to carry out the mandate and responsibilities of CLBC.

Freedom of Information and Protection of Privacy Act (FOIPPA): Provincial legislation that provides the legal context for the accountability of public bodies, including CLBC, as regards to information sharing and protecting personal privacy.

Informed Consent: A person is made aware of the decision or choice to be made; understands the possible consequences of giving or not giving consent, including for instance the purpose for which released information may be used; and then consents voluntarily.

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 information, whether accidental or deliberate.

Information Security Officer (ISO): A designated position within CLBC with overall responsibility for policies and compliance related to the security of information assets contained in and related to CLBC information technology systems. This position is also sometimes called the information custodian. The Director, Information Technology, is CLBC’s Information Security Officer.

Need-to-Know: The legitimate requirement to know, access or possess personal information that is critical to the performance of an authorized, assigned mission.

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 licence 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 Impact Assessment: A Privacy Impact Assessment is an assessment of a current or proposed initiative (a system, enactment, project, program or activity) to evaluate privacy impacts, including compliance with the privacy protection responsibilities under 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 Manager, Quality Assurance is CLBC's Privacy Officer.

Privacy of Personal Information: The fundamental right of individuals to determine for themselves when, how and to what extent their personal information is collected, used and communicated to others.

Service Provider: A person or an independent organization under contract with CLBC to deliver supports and services to individuals and/or families. This term is also utilized in situations where a contract has not yet been issued such as during an approval or procurement process.

Third Party: A person or organization other than the person or organization requesting the information.

3. POLICY

CLBC protects the privacy and confidentiality of personal information of individuals and their families, and of CLBC employees. Individuals, their families and employees can expect that their personal information is used only for consistent purposes. CLBC applies the following practices in all actions and decisions involving personal information of individuals, families and CLBC employees:

- Limiting the collection of personal information to that which is relevant and necessary to the purpose for which it was collected;
- Obtaining personal information with the knowledge and consent of the individual;
- Maintaining personal information in an accurate, complete and up-to-date manner;
- Using personal information only for purposes which reflect the original intent of collection;
- Keeping personal information confidential, other than for the specified purposes for which it was collected, except with the informed consent of the individual or as required by law;
- Accessing and using personal information only on a need-to-know basis;
- Protecting personal information with security safeguards against risk of loss, unauthorized access, destruction, use, modification or disclosure of such information;
- Retaining personal information for a specified period of time as required by law or policy;
- Maintaining openness about policy and practices with respect to personal information, including what kinds of information the organization has, where it is stored and how it is used;
- Ensuring employees are not suspended, demoted, disciplined, harassed or otherwise disadvantaged if they report an infraction under the whistle bower protection section of the *Freedom of Information and Protection of Privacy Act* (FOIPPA) or the CLBC policy on ethical reporting;
- Informing individuals of the process for obtaining or correcting their personal information; and
- Accounting publicly for compliance measures related to these practices.

CLBC requires that service providers comply with the *Privacy Protection Schedule* which forms part of the Terms and Conditions of their contract, in order to protect the privacy and confidentiality of personal information of individuals supported by CLBC.

CLBC complies with FOIPPA Privacy Impact Assessment (PIA) requirements by ensuring PIAs are completed during the development of any new project, program, activity or system including Information Sharing Agreements and Data-linking initiatives, as well as when making significant changes to an existing one. The PIA must be fully completed before implementation.

CLBC provides detailed policy direction on specific aspects of the privacy and confidentiality of personal information through a suite of privacy policies and policy tools listed in *Appendix 1* of this policy.

4. PROCEDURES

4.1 All Staff

- Comply with the *Standards of Conduct for Community Living BC Employees* and with the specific privacy related policies and policy tools listed in *Appendix 1*.
- Consult with their Integrated Service Manager for guidance as required, and with the Manager, Quality Assurance as directed by their Integrated Service Manager.
- Report any actual or suspected breach of privacy of personal information to their Integrated Service Manager and the Manager, Quality Assurance.
- Assist individuals, families and service providers with questions about privacy, confidentiality and information sharing.

4.2 Integrated Service Managers

- Ensure that staff are aware of and comply with all CLBC privacy policies and practices.
- Advise the Manager, Quality Assurance of any gaps in privacy policy or practices.
- Consult with the Manager, Quality Assurance with questions about privacy policies and practices, and for guidance regarding issues or complaints that involve privacy.
- Consult with the Manager, Quality Assurance around any proposed information sharing to determine the need for a PIA and to participate as needed in PIAs.

4.3 Manager, Quality Assurance

- Acts as CLBC's designated Privacy Officer, with overall responsibility and accountability for CLBC privacy policies and related compliance and quality assurance processes.
- Oversees development and implementation of CLBC privacy policies and practices.
- Ensures that existing and new CLBC policies address FOIPPA privacy requirements.
- Ensure directors and Integrated Service Managers are aware of the PIA requirements of the FOIPPA.
- Ensures completion of PIAs and submits them to the Office of the Chief Information Officer where required.
- Consult with Integrated Service Managers regarding issues related to the privacy and security of personal information.
- Ensures CLBC maintains adequate systems for preventing information incidents including privacy breaches.
- Manages the response to information incidents including privacy breaches.
- Consults and liaises with the Office of the Chief Information Officer as needed.

4.4 Director, Human Resources

- Ensures that personnel policies and practices reflect the rights of staff and applicants to privacy and confidentiality as required by FOIPPA.

4.5 Director, Information Technology

- Ensures that CLBC information systems are compliant with FOIPPA, the expectations of the Office of the Chief Information Officer and with CLBC information security policies.
- Identifies new areas where information security policies may be required.
- Manages the response to information incidents including privacy breaches of electronic systems in conjunction with the Manager, Quality Assurance.

5. DOCUMENTATION

5.1 Required documentation is completed as described in the specific privacy policies and in the *Documentation and Recording Policy: Individual Records*.

6. PRACTICE

6.1 The protection of the privacy and confidentiality of personal information is a core element of the CLBC organizational culture, reflecting the values of trust and respect in our relationships with the people we support. Staff are expected to integrate this element into their everyday practice and relationships with each other, with individuals and families, and with third parties.

6.2 Staff are expected to become familiar with the *CLBC Privacy Guidelines*. These guidelines provide background, an overview of privacy legislation affecting CLBC and service providers, and a summary of the key aspects of CLBC privacy policy and practice. They are written in straightforward language and are suitable for sharing with individuals and families or with service providers, when explaining the CLBC approach to privacy or answering questions.

6.3 There may be situations where an alternate decision maker, usually a Committee, may act for the individual in matters regarding the individual's personal information. See the *Role of Formal and Informal Representatives Policy*, and/or consult with the Manager, Quality Assurance for direction.

7. REFERENCES

BC Freedom of Information and Protection of Privacy Act

CLBC Privacy Guidelines

CLBC Standards of Conduct for Community Living British Columbia Employees

CLBC Confidentiality and Information Sharing Policy

CLBC Documentation and Recording Policy: Individual Records

CLBC Role of Formal and Informal Representatives Policy

Information about completing Privacy Impact Assessments:

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

Appendix 1: CLBC Privacy Policy Suite Operational Privacy Policies and Tools

Access to Personal Information for Research Purposes Policy	<ul style="list-style-type: none"> ○ Conditions where personal information can be used in research
Confidentiality and Information Sharing Policy	<ul style="list-style-type: none"> ○ Sharing personal information with or without consent ○ Documenting consent and release of information
Information Incidents including Privacy Breaches Policy	<ul style="list-style-type: none"> ○ Information regarding what to do, including reporting requirement in case of an information incident or privacy breach
Protection of Information Policy	<ul style="list-style-type: none"> ○ Physical/electronic safeguards for protecting privacy of information in CLBC offices/systems and when working off site.
Right to Access Personal Information Policy	<ul style="list-style-type: none"> ○ Providing access for individuals to their personal information ○ Enabling individuals to correct or update their personal information
Use of E-mail and Fax Policy	<ul style="list-style-type: none"> ○ Limitations on transmission of personal information through e-mail and fax
Use of Social Media Policy	<ul style="list-style-type: none"> ○ Appropriate use of internet and social media for staff in work situations

Human Resources Privacy Policies and Tools

Employee Personal Information Statement	<ul style="list-style-type: none"> ○ Privacy of employee's personal information ○ How and when employees personal information may be shared
Internet and Communications Technology Use Agreement	<ul style="list-style-type: none"> ○ Agreement signed by employees prior to accessing CLBC and government information and communications technologies
Standards of Conduct for Community Living BC Employees	<ul style="list-style-type: none"> ○ Expectations of CLBC employees ○ Agreement signed by the employee

Related Policies

Documentation & Recording Policy: Individual Records	<ul style="list-style-type: none"> ○ How to collect personal information ○ Issuing a privacy notice when collecting information
Ethical Reporting Policy	<ul style="list-style-type: none"> ○ Process for staff to report ethical issues and CLBC

	response
Information Security Policy (to be updated)	<ul style="list-style-type: none"> ○ Overarching framework providing information security controls throughout CLBC.
Legal Requirements Policy	<ul style="list-style-type: none"> ○ Situations where these may be a legal requirement to share personal information
Role of Formal and Informal Representatives Policy	<ul style="list-style-type: none"> ○ Defines and describes the roles of authorized representatives of individuals

Privacy Tools Affecting Service Providers

Schedule E: Privacy Protection	<ul style="list-style-type: none"> ○ Requirements for service providers regarding privacy of personal information of individuals supported by CLBC ○ Forms part of service provider's contract , Terms and Conditions
--------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------