Policy

APPROVED

Privacy

Purpose

To establish requirements and responsibilities for the lawful collection, access, use, disclosure, storage and disposal of personal information by BCLC.

To establish a privacy program for BCLC that will provide oversight for administering BCLC's compliance with its requirements under FIPPA.

Scope

This policy applies to full-time, part-time, temporary and on-call employees of BCLC. It also applies to third parties if required by BCLC.

This policy applies to all Personal Information in BCLC's custody or under BCLC's control, and all transactions conducted or authorized by BCLC that involve the collection, use, retention, disclosure and destruction of Personal Information.

Policy Statement

BCLC is committed to protecting the personal information in our custody or under our control. BCLC shall collect, use, retain, disclose, safeguard and dispose of Personal Information in accordance with all applicable laws.

Context

LEGAL AND POLICY FRAMEWORK

Personal privacy is a right protected by the Government of British Columbia through legislation, policies and best practices. The *Freedom of Information and Protection of Privacy Act* (FIPPA), British Columbia outlines the accountability and requirements of all B.C. public bodies for the protection of privacy in the form of personal information. As a public body, BCLC must comply with the provisions of FIPPA when collecting, accessing, using, disclosing, storing and disposing of personal information.

Every individual's personal information is a valuable asset that should be treated with care and respect. In the course of its normal business activities BCLC collects many different types of personal information from many individuals. In some circumstances those with whom BCLC has contracted, such as casino service providers, may be required by BCLC to collect personal information on BCLC's behalf.

From time to time BCLC may need to collect sensitive pieces of personal information, such as a driver's license number or banking information. This type of personal information is considered sensitive because it can be used for identity theft (when someone's personal identity information is stolen) and identity fraud (when someone

else's information is used to commit financial fraud or some other kind of crime). Another example of sensitive personal information is the name and records associated with a self-excluded individual. The public has a heightened awareness and concern about how sensitive personal information is used and disclosed.

BCLC is committed to operating within a privacy framework that is responsive to these concerns. This framework is based on the three principles of fairness, accountability and accessibility. These principles need to be understood and acted upon by all BCLC employees who collect, use or disclose personal information as part of their jobs.

Policy Details

BCLC's commitment to privacy is based upon three pillars – fairness, accountability and accessibility. Additional policies, procedures and guidelines are developed or revised as required to support BCLC's compliance with FIPPA and the principles and associated activities set out below.

FAIRNESS

BCLC strives to use fair information practices. It is the policy of BCLC to:

- Provide a Privacy Notice to individuals upon the collection of Personal Information.
- Limit the collection of Personal Information to that which is necessary for operating a BCLC program or activity, expressly authorized by law, or required for the purposes of law enforcement.
- Publish or disseminate Personal Information only with prior consent of the individual or unless required or provided for by law.
- Manage the retention of records containing personal information in accordance with existing legislation and policy.
- Include Privacy Protection Schedules in all contracts that involve exchanging sensitive Personal Information outside of BCLC.

ACCOUNTABILITY

BCLC is accountable for the management of Personal Information in our Custody or under our Control. It is the policy of BCLC to:

- Carry out Privacy Impact Assessments for proposed systems, projects, programs and activities that may involve the collection or use of Personal Information.
- Send Information Privacy and Security Assessments for key initiatives to the Office of the Information and Privacy Commissioner for review, when appropriate.
- Establish policies, procedures and controls to appropriately safeguard Personal Information throughout its life cycle.

APPROVED

Privacy

- Provide mandatory privacy training to employees and require the completion of training on initial employment and as required thereafter.
- Develop and maintain a directory of all BCLC Personal Information Banks, in accordance with requirements outlined in FIPPA.
- Assign accountability for the management of Personal Information to appropriate Directors.
- Investigate and report Privacy Breaches in accordance with established procedures designed to ensure unauthorized disclosures of personal information are identified and contained, affected individuals are notified, and the underlying causes of the breach are addressed.

ACCESSIBILITY

BCLC aims to be open about our privacy policies and practices. It is the policy of BCLC to:

- Provide individuals with access to their own personal information in accordance with established processes and subject to the provisions of FIPPA.
- Provide individuals about whom we have personal information with an answer, in a timely manner, to questions about how their information will be used.

Privacy and Playnow.com

Our commitment to PlayNow.com players is outlined in the Player Privacy Policy. Before implementing any changes to PlayNow that may affect the collection, use, retention, disclosure, or destruction of Personal Information, a Privacy Impact Assessment must be undertaken in accordance with the Information Privacy and Security Assessment procedure.

Compliance

Employees must adhere to all privacy policies and rules of conduct related to the collection, use, retention, disclosure, security and disposal of personal information and may be subject to administrative, civil, or criminal sanctions if they willfully or negligently disclose Personal Information to unauthorized persons. Each case will be handled on an individual basis with full review of all pertinent facts. Severity of the violation will determine action taken.

Employees are responsible for seeking guidance from their manager or the Director of Information Privacy and Security if they are unsure as to the extent of the compliance requirements.

APPROVED

Privacy

Definitions

Contact Information	Is information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual.
Control (of information)	Means the power or authority to manage the information throughout its life cycle, including restricting, regulating and administering its use or disclosure.
Custody (of information)	Means having physical possession of information. Physical possession normally includes responsibility for access, managing, maintaining, preserving, disposing, and providing security.
Personal Information	Is recorded information about an identifiable individual, other than Contact Information.
Personal Information Bank	Means a collection of Personal Information that is organized or retrievable by the name of an individual or by an identifying number, symbol or other particular assigned to an individual.
Privacy Breach	Means unauthorized access to or collection, use, disclosure or disposal of Personal Information. Such activity is "unauthorized" if it occurs in contravention of Part 3 of FIPPA.
Information Privacy and Security Assessment (IPSA)	Means an assessment that is conducted to determine if a business process, application or information system meets the requirements of Part 3 of FIPPA and is designed and implemented in accordance with BCLC's privacy and security standards.
Privacy Notice	Means the statement required under s. 27(2) of FIPPA informing an individual of: • The purpose for collecting his/her Personal Information; • the legal authority for collecting his/her Personal Information; and • the title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection of his/her Personal Information.

APPROVED

Privacy

Policy Ownership

Policy Owner	Director, Information Privacy
Approving Body	Vice President, Corporate Security and Compliance

Revision History

Version	Effective	Approved by	Amendment
3.1	Jan 29, 2015	Vice President, Corporate Security & Compliance	Minor amendment to footer text. This document was re-classified from 'Internal' to 'Public' in order to comply with a directive from the Public Sector Employers' Council. An exemption to policy approval requirements was made due to exceptional circumstances.
3.0	Aug 19, 2013	Vice President, Corporate Security & Compliance	References to Director of Privacy changed to Director of Information Privacy and Security to reflect organizational change. Changes made to reflect integration of privacy and security assessment processes.
2.0	Mar 26, 2012	Director, Privacy	Revised to reflect amendments to FIPPA with respect to Privacy Impact Assessments.
1.1	Jan 24, 2011	Director, Privacy	References to Privacy Compliance Manager changed to Director of Privacy to reflect organizational change.
1.0	Apr 12, 2010	Vice President, Corporate Security & Compliance	Inaugural.