Communications

Corporate Policy

6.14 Privacy Policy

October 28, 2019

1. PRIVACY POLICY

Effective Date: February 12, 2020

2. POLICY OBJECTIVE

The objectives of this policy are to ensure:

- The NSLC complies with all applicable privacy laws governing personal information in its custody or control; and
- All individuals working within, for or on behalf of the NSLC are fully accountable for protecting personal information and respecting the privacy rights of individuals, in accordance with legislation when carrying out their duties.

3. SCOPE

This policy applies to:

- Individuals employed by the NSLC on a permanent, temporary, part-time, or contract basis;
- The NSLC Board of Directors;
- All third-party service providers of the NSLC to the extent that they access, handle or store personal information on behalf of the NSLC as part of their duties;
- All personal information in the custody or control of the NSLC:
    - in all recorded formats, digital or paper, and in all storage locations including personal devices;
    - in all of the NSLC's business functions, services and programs including but not limited to the NSLC's beverage alcohol and cannabis lines of business; and
    - related to employees, customers, clients, members of the public, and other individuals.

4. DEFINITIONS

DIGITAL PRIVACY ACT: An amendment to The *Personal Information Protection and Electronics Document Act* (PIPEDA) that imposes privacy breach notification and record keeping requirements for every organization that collects, uses and discloses personal information in the course of commercial activity.

Approval date: February 12, 2020	Effective date: February 12, 2020
Approved by: Board of Directors	Administrative update: October 28, 2019

FOIPOP ACT: The *Freedom of Information and Protection of Privacy Act* (Nova Scotia) and the related Regulations.

INFORMATION AND PRIVACY COMMISSIONER: An independent ombudsman appointed by the Governor in Council for a term of five to seven years. The Office of the Information and Privacy Commissioner (OIPC) accepts appeals (referred to as "requests for review") and investigates privacy complaints received pursuant to the FOIPOP Act and the PRO Act.

PERSONAL INFORMATION: As per Section 3(1)(i) of the FOIPOP Act, personal information means "recorded information about an identifiable individual", including [but not limited to]:

i. the individual's name, address or telephone number,
ii. the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations,
iii. the individual's age, sex, sexual orientation, marital status or family status,
iv. an identifying number, symbol or other particular assigned to the individual,
v. the individual's fingerprints, blood type or inheritable characteristics,
vi. information about the individual's health-care history, including a physical or mental disability,
vii. information about the individual's educational, financial, criminal or employment history,
viii. anyone else's opinions about the individual,
ix. the individual's personal views or opinions, except if they are about someone else

PIIDPA: The *Personal Information International Disclosure Protection Act* (Nova Scotia).

PIPEDA: The *Personal Information Protection and Electronics Document Act* (Canada).

PRIVACY BREACH: The intentional or unintentional unauthorized collection, use, disclosure, disposal, modification, reproduction, access, or storage of personal information that is in violation of the FOIPOP Act or PIIDPA or other applicable privacy law.

PRIVACY IMPACT ASSESSMENT (PIA): A due diligence exercise that: (i) identifies and addresses potential risks to the privacy of individuals' personal information that may arise in an existing system, project, program or activity of the NSLC or a change thereto; and (ii) helps to ensure the NSLC's compliance with this policy, the FOIPOP Act and PIIDPA.

PRIVACY NOTICE: A notification, electronic or otherwise, to individuals about: the purpose for which personal information is collected (i.e., principally how the information is intended to be used); the authority for such collection; and the contact information for the NSLC Privacy Officer or another individual within the NSLC who can answer questions about the collection, including a reference to NSLC's Privacy Statement where more information about the NSLC's collection practices may be found.

PRIVACY FRAMEWORK: A program encompassing privacy controls and processes, tools for fulfilling privacy obligations and managing privacy risks, a strategy and materials for providing awareness and education of privacy best practices through training, and methods for monitoring performance.

THIRD-PARTY SERVICE PROVIDER: An organization, business or individual that provides services to the NSLC (e.g., IT, consulting, warehousing, product delivery services, etc.).

5. POLICY STATEMENT

The Nova Scotia Liquor Corporation (NSLC) is committed to protecting the personal information that it collects, uses, discloses and maintains, and to upholding the privacy rights of all customers, employees and other individuals whose personal information is held or controlled by the NSLC, in accordance with the requirements of the *Freedom of Information and Protection of Privacy Act* (FOIPOP Act), the *Personal Information International Disclosure Protection Act* (PIIDPA), and other applicable legislation. The NSLC will also consider the requirements of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and related *Digital Privacy Act*, and the *Canada Anti-Spam Legislation* (CASL) when carrying out its activities that are commercial in nature.

6. POLICY REQUIREMENTS

a) Accountability for Personal Information

The NSLC is accountable for personal information in its custody and under its control, which includes ensuring appropriate collection, use, disclosure, retention, storage, and protection, in accordance with applicable privacy legislation. The NSLC is accountable for implementing and maintaining a Privacy Framework to facilitate consistently meeting its privacy obligations, adhering to privacy principles and managing privacy risks effectively over time.

The NSLC Privacy Officer is accountable for overseeing the NSLC's compliance with privacy legislation, through the Privacy Framework.

The NSLC's accountability also extends to personal information that is collected, used (e.g., handled or processed), accessed or stored on its behalf by third-party service providers. The NSLC will use contractual or other means to provide a comparable level of protection for personal information being processed or accessed by a third party on its behalf.

All individuals subject to this policy will:

- Adhere to this Privacy Policy and any supporting NSLC policies and procedures when collecting, using, disclosing, storing, handling, retaining, and disposing of personal information; and
- Formally acknowledge (in writing), upon hire or upon contract signing, that they have reviewed, understand and agree to comply with the NSLC's privacy policies.

b) Privacy Impact Assessments

- The use of privacy impact assessments will be incorporated as a required component of the NSLC project management, IT planning, and new business development processes.
- Managers (including Project Managers) will notify the NSLC Privacy Officer upon development of or significant change to any system, project, program, service or activity that involves the collection, use, storage, disclosure or access of personal information, to obtain an opinion on whether a PIA is necessary.
- PIAs will be reviewed by the Privacy Officer to ensure compliance with applicable privacy legislation and this policy.
- Risks documented in PIAs will be managed in a risk log maintained by the Privacy Officer. It is the responsibility of the Privacy Officer to ensure risks are either mitigated, or that the business reason for not mitigating risks is clearly documented in the risk log.
- PIAs will be approved by the business owner of the program, service or line of business, before any personal information is collected, used, stored, disclosed or accessed.

c) Consent

- Meaningful consent is required for the collection, use and disclosure of personal information for NSLC activities that are commercial in nature, i.e. retail and wholesale business activities.
- The NSLC has processes in place to manage changes in individuals' consent preferences (e.g. opt-in or opt-out), where applicable and permitted by law. Any requests to change an individual's consent preferences will follow the NSLC's consent management process.
- Consent will be obtained prior to using an individual's personal information to send Commercial Electronic Messages (CEMs). Canada's Anti-Spam Law (CASL) requires any CEMs sent by the NSLC to its customers or members to follow the consent requirements in the statute, identify NSLC as the sender of the message, and include contact information and an unsubscribe mechanism.
- Written consent will be obtained for the use or disclosure of personal information for a purpose different than that for which the information was obtained or compiled, or for a use that does not have a reasonable and direct connection to that purpose, unless the proposed use or disclosure is provided pursuant to the FOIPOP Act or any other enactment.

d) Collection of Personal Information

No personal information may be collected by the NSLC or on the NSLC's behalf unless:

- The collection of the personal information is authorized or required by law; or
- The information relates directly to and is necessary for an operating program or activity of the NSLC.

When collection is authorized as above, the NSLC will, before collecting the personal information:

- Identify the specific purpose(s) for which each type of personal information is being collected;
- Post a privacy notice at each point where personal information is collected directly from individuals, where it is likely to come to their attention. The content of the notice should include the purpose for the collection of the personal information and the legal authority for the proposed collection, as determined by the business owner in consultation with the NSLC Privacy Officer. It should also identify the position title and contact information for the NSLC Privacy Officer or other individual within the NSLC who can answer questions about the collection of the information.
- Take all necessary steps to collect only as much personal information as is needed to accomplish the identified purpose(s) for which the information is being collected.

e) Use and Disclosure of Personal Information

Personal Information may only be used or disclosed:

- In accordance with the FOIPOP Act or as provided pursuant to any other enactment;
- If the individual the information is about has identified the information and provided written consent;
- For the purpose for which the information was obtained or compiled, or for a use that has a reasonable and direct connection to that purpose;
- For the purpose of complying with an enactment or with an agreement made pursuant to an enactment;
- For the purpose of complying with a subpoena, warrant or court order;
- To collect a debt from or make a payment to an individual; or
- If otherwise authorized by the FOIPOP Act.

The NSLC will:

- Take reasonable steps to only use or disclose the minimum amount of personal information required for the immediate, valid purpose; and
- Limit access to personal information on a "need to know" basis, ensuring that individuals are only permitted to access and use the minimum amount of personal information necessary to carry out their roles within the NSLC for each identified and authorized purpose.

f) Retention and Destruction of Personal Information

Personal information will be retained only as necessary for the fulfillment of the identified and authorized purposes or as required by law. As a public body, the NSLC will comply with the provisions of the *Government Records Act* and ensure electronic and paper records related to the collection of personal information for the NSLC's operations are retained and disposed of in accordance with the STAR/STOR government retention schedules.

NSLC will also implement procedures to ensure that personal information that:

- Has been used to make a decision about an individual is retained for at least one year after using it so that the individual has a reasonable opportunity to obtain access to it;
- Is no longer required to fulfill the purposes identified at the time of collection is securely destroyed, erased or de-identified so that unauthorized parties do not gain access to the information. Personal information held on electronic media will always be disposed of in accordance with industry standard methods. Personal information contained in hard copy format will be disposed of in such manner that no personal information can be derived from these records following their disposal (e.g. using a cross cut shredder).

g) Access and Storage of Personal Information Outside of Canada

The NSLC will ensure personal information under its custody or control is accessed and stored in accordance with PIIDPA. Controls will be included in all contracts and business arrangements with third party service providers that handle personal information on the NSLC's behalf to verify service providers' compliance with PIIDPA.

h) Accuracy

- The NSLC will take reasonable steps to ensure personal information is accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used, and to minimize the possibility that inaccurate or incomplete information may be used to make a decision that directly affects an individual;
- NSLC will make reasonable efforts to collect personal information directly from the individual to whom the information relates, unless otherwise permitted by law;
- Requests for correction of personal information held by the NSLC will be directed to the Privacy Officer and should be made in writing.

i) Safeguarding Personal information

All employees will protect personal information against such risks as unauthorized access, collection, use, disclosure or disposal using reasonable security arrangements. The security arrangements will include appropriate technical, administrative and physical safeguards that are chosen based on the sensitivity of the information that has been collected; the amount, distribution, and format of the information; and the method of storage.

The NSLC will also ensure that service providers are required to adhere to the NSLC's legal obligations related to appropriate handling and safeguarding of personal information and this privacy policy by including appropriate contractual clauses in written agreements with its service providers. The NSLC will also review and assess the ability of its service providers to comply with these measures prior to engaging them and implement auditing and other controls to verify compliance with the required safeguards.

j) Privacy Breach

- The NSLC will maintain a privacy breach management protocol to be followed in the event of a known or suspected privacy breach to ensure an effective and timely response to privacy breaches, in accordance with legal requirements;
- Employees will immediately report any actual or suspected breach of privacy to their immediate supervisor and the NSLC Privacy Officer;
- All privacy breaches shall be contained and investigated in accordance with the privacy breach protocol;
- The NSLC shall track and record incidents of all breaches involving personal information and provide notification of privacy breaches to the effected individuals where there is a real risk of significant harm, pursuant to the privacy breach protocol.

k) Openness

NSLC will be open about its policies and practices with respect to managing personal information and will make specific information about its information practices readily available to its customers, clients and the public by creating and maintaining a Privacy Statement. The Privacy Statement describes the type of personal information held by the NSLC and its service providers, why it is collected and how it is used, disclosed, retained, and protected. The privacy statement also describes individuals' rights and choices when they provide personal information to the NSLC, including but not limited to the means by which an individual can gain access to his or her personal information held by the NSLC and to whom complaints or inquiries can be directed.

The NSLC will regularly review the privacy statement to ensure continued alignment with its information practices and applicable privacy legislation, and update it as needed based on any changes to the way the NSLC collects, uses, discloses or protects personal information.

l) Individual Access

- Individuals have the right to request access to or correction of their personal information and to examine or receive a copy of their personal information maintained by the NSLC, subject only to limited exceptions outlined in FOIPOP, by making a request to the NSLC FOIPOP Administrator; and
- Where access or correction is refused in part or in whole, in accordance with the exemptions outlined in FOIPOP, individuals will be provided with the reasons for the refusal and informed of their right to complain about the NSLC's decision to the Nova Scotia Office of the Information & Privacy Commissioner.

m) Complaints

- Upon receipt of a privacy complaint, employees will immediately refer the complaint to the NSLC Privacy Officer.

- All complaints shall be investigated by the NSLC in accordance with the privacy complaints procedure.
- The NSLC will respond to the complainant within a reasonable time frame, and where possible, within thirty calendar days.
- If an individual is not satisfied with the response from NSLC, they will be informed of their right to complain to the Office of the Information & Privacy Commissioner or the Privacy Commissioner of Canada.

7. POLICY GUIDELINES

To support the administration of this policy, the NSLC may develop written procedures to provide guidance in specific areas. These procedures will be in alignment with the direction of this policy and the Privacy Framework.

8. ACCOUNTABILITY

a) Employees

All employees are required to:

- Know and understand their obligations under this policy and other NSLC privacy policies and comply with these policies and any supporting privacy procedures;
- Complete all required privacy training;
- Respect the confidentiality of personal information and the privacy rights of individuals and make reasonable efforts to protect personal information, as required under this policy;
- Immediately report any breaches of privacy and any privacy complaints to their immediate supervisor and the NSLC Privacy Officer; and
- Manage personal information in a manner that is consistent with this policy and other privacy polices and procedures established by the NSLC.

b) Managers

In addition to the responsibilities noted above, managers are required to:

- Ensure that staff are aware of this policy and any related NSLC privacy policies and procedures;
- Hold staff accountable for compliance with the NSLC's privacy policies as part of their employment duties;
- Ensure all staff attend required privacy training;
- Ensure PIAs are completed, where required, for new projects, programs, and systems (or significant changes thereto) involving the planned collection, use, disclosure, and storage of personal information, in consultation with the NSLC Privacy Officer; and
- Ensure privacy risks associated with new and existing projects, programs and systems are being assessed and appropriately mitigated effectively and in a timely manner.

c) Senior Leadership Team

In addition to the employee and manager responsibilities noted above, the members of the NSLC Senior Leadership Team are required to:

- Promote and champion the implementation and of the Privacy Framework within the NSLC;
- Provide oversight of the Privacy Framework and incorporate discussions about privacy in periodic reviews and reporting of organizational performance and risks to the NSLC Board of Directors;
- Review the NSLC Privacy Policy and significant changes thereto and recommend it for approval ;
- Approve agreements and contracts related to service providers' handling of personal information within Canada.
- Keep informed about privacy risks and legislative compliance requirements impacting the NSLC.

d) NSLC President and Chief Executive Officer

In addition to the Senior Leadership Team responsibilities noted above, the NSLC President and Chief Executive Officer (CEO) is accountable to:

- Oversee the application of this policy by the NSLC; and
- Approve agreements and contracts related to service providers' handling of personal information regarding provisions prohibiting the storing or access to personal information outside Canada, or granting permission for the storage or access outside of Canada in accordance with PIIDPA, where the PIIDPA requirements have been met.

e) NSLC Board of Directors

The NSLC Board of Directors members are required to:

- Know and understand their obligations under this policy;
- Receive reports on the NSLC's progress in implementing and maintaining the Privacy Management Framework as part of their role in overseeing organizational performance and risk.

f) NSLC Privacy Officer

The NSLC Privacy Officer is responsible to:

- Provide advice and guidance to the organization with respect to the management of personal information within the NSLC;
- Lead the development of the NSLC Privacy Framework, monitor and assess progress in implementing the Privacy Framework, and report on progress to the Senior Leadership Team;
- Ensure the NSLC Privacy Framework is updated and kept current, based on:
    - Changes in the business environment or the NSLC's legal or regulatory framework;
    - The outcome of PIAs, audits, or other privacy or security risk assessments;
    - Recommendations and lessons learned from post-breach or complaint reviews; and
    - Emerging best practices;

- Advise managers on PIA requirements for planned initiatives, and how to incorporate PIAs and other privacy risk management tools and approaches into NSLC project management, IT planning and new business development processes;
- Provide tools and guidance to support managers and employees in identifying the requirement for and conducting or participating in privacy impact assessments (PIAs) within their job activities;
- Review all PIAs to ensure compliance with privacy legislation and this policy;
- Maintain a risk log ensuring all unmitigated risks are documented with business decisions and that mitigated risks, and associated measures taken to mitigate, are documented.
- Receive, evaluate, and lead the resolution of privacy incidents, breaches and complaints in accordance with this policy and the Privacy Breach Protocol;
- Oversee the monitoring and report on the NSLC's compliance with this policy; and
- Oversee implementation and periodically review and update a privacy training program for employees, managers, executives and the Board of Directors.

9. COMPLIANCE AND MONITORING

Employees, managers, and service providers are responsible to comply with this policy. NSLC will monitor compliance and any non-compliance with this policy may be subject to disciplinary action, up to and including termination.

10. REFERENCES AND RELATED DOCUMENTS

- *Freedom of Information and Protection of Privacy Act* and Regulations
- *Privacy Review Officer Act*
- *Personal information International Disclosure Protection Act* and Regulations
- *Canada Anti-Spam Legislation* and Regulations
- *Personal Information Protection and Electronic Documents Act* and Regulations
- *Digital Privacy Act* and draft Regulations
- Privacy Breach Management Protocol
- Information Security Policy
- Information Security Incident Management Policy
- Enterprise Risk Management Policy