



Gulf of Georgia Cannery Society

Personal Information Protection Policy

At the Gulf of Georgia Cannery Society, we are committed to providing our stakeholders with exceptional service. As providing this service involves the collection, use and disclosure of stakeholders' personal information, protecting personal information is one of our highest priorities.

This policy provides for the protection of personal information as required by British Columbia's *Personal Information Protection Act* (PIPA). PIPA sets out the ground rules for how B.C. businesses and not-for-profit organizations may collect, use and disclose personal information.

This Personal Information Protection Policy outlines the principles and practices we follow in protecting stakeholders' personal information. Our privacy commitment includes ensuring the accuracy, confidentiality, and security of stakeholder personal information and allowing our stakeholders to request access to, and correction of, their personal information.

Definitions

Personal Information – information about an identifiable *individual*, including name, home address, phone number, email address, birthdate, credit card information, partnership status, medical information, gender, educational history, employment history and, for employees, also includes social insurance number and income. Personal information does not include contact information (described below).

Contact information – information that would enable an individual to be contacted at a *place of business* and includes name, position name or title, business telephone number, business address, business email or business fax number. Contact information is not covered by this policy or PIPA.

Stakeholder – any current, past or prospective member, volunteer, donor, employee, or client of the Gulf of Georgia Cannery Society. Stakeholders do not include businesses, contractors or vendors with whom the Society conducts business.

Privacy Officer – the individual designated responsibility for ensuring that the Society complies with this policy and PIPA.

Policy 1 – Collecting Personal Information

- 1.1 We communicate the purposes for which personal information is being collected, either orally or in writing, before or at the time of collection, unless the purposes for collecting personal information are obvious and the individual voluntarily provides his or her personal information for those purposes.
- 1.2 We only collect information necessary to fulfill the following purposes:
 - The purchase of goods or services, including credit card and banking information;
 - Conduct raffles or promotional prize draws;
 - Enrol a member for contact purposes;
 - Enrol a volunteer for contact and emergency purposes;
 - Provide a donor a tax receipt;
 - Enrol an employee for payroll, contact and emergency purposes;
 - Document artifact donations.

Policy 2 – Consent

- 2.1 We obtain stakeholder consent to collect, use or disclose personal information (except where, as noted below, we are authorized to do so without consent).
- 2.2 Consent can be provided or it can be implied where the purpose for collecting using or disclosing personal information is considered obvious and the stakeholder voluntarily provides personal information for that purpose.
- 2.3 Consent may also be implied where a stakeholder is given notice and reasonable opportunity to opt-out of his or her personal information and the stakeholder does not opt-out.
- 2.4 Subject to certain exceptions (e.g. the personal information is necessary to provide the service or product, or the withdrawal of consent would frustrate the performance of a legal obligation), stakeholders can withhold or withdraw their consent for the Society to use their personal information in certain ways. A stakeholder's decision to withhold or withdraw their consent to certain uses of personal information may restrict our ability to provide a particular service or product. If so, we will explain the situation to assist the stakeholder in making the decision.
- 2.5 We may collect, use or disclose personal information without the stakeholder knowledge or consent in the following limited circumstances:
 - When the collection, use or disclosure of personal information is required by law;
 - In an emergency that threatens an individual's life, health, or personal security;
 - When we require legal advice from a lawyer;
 - For the purposes of collecting a debt;
 - To protect ourselves from fraud;
 - To investigate a breach of an agreement or a contravention of law.

Policy 3 – Using and Disclosing Personal Information

- 3.1 We use or disclose member personal information only where necessary to fulfill the purposes identified at the time of collection.
- 3.2 We do not use or disclose personal information for any additional purpose unless we obtain consent to do so.
- 3.3 We do not sell personal information to other parties.

Policy 4 – Retaining Personal Information

- 4.1 If we use an individual's personal information to make a decision that directly affects the individual, we retain that personal information for at least one year so the individual has a reasonable opportunity to request access to it.
- 4.2 Subject to policy 4.1, we retain personal information only as long as necessary to fulfill the identified purposes or a legal or business purpose.

Policy 5 – Ensuring Accuracy of Personal Information

- 5.1 We make reasonable efforts to ensure personal information is accurate and complete.
- 5.2 Stakeholders may request correction to their personal information in order to ensure its accuracy and completeness. A request to correct personal information must be made in writing and provide sufficient detail to identify the personal information and the correction being sought.

Policy 6 – Securing Personal Information

- 6.1 We are committed to ensuring the security of personal information in order to protect it from unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks.
- 6.2 The following security measures ensure that personal information is appropriately protected:
 - Electronic information is stored on secure servers, with password protected access;
 - Paper information is stored in locked file cabinets with restricted key access.
- 6.3 We immediately dispose of full credit card or bank account information after use.
- 6.4 We use appropriate security measures when destroying personal information such as document shredding and deletion of electronic database information.
- 6.5 We continually review and update our security policies and controls as technology changes to ensure ongoing personal information security.

Policy 7 – Providing Stakeholder Access to Personal Information

- 7.1 Individual stakeholders have a right to access their personal information, subject to limited exceptions (listed in Section 23 of the Personal Information Protection Act).
- 7.2 Upon request, we tell stakeholders how we use their personal information and to whom it has been disclosed if applicable.

- 7.3 We make the requested information available within 30 business days, or provide written notice of an extension where additional time is required to fulfill the request.
- 7.4 If a request is refused in full or in part, we notify the member in writing, providing the reasons for refusal and the recourse available to the member.

Policy 8 – The Role of the Privacy Officer

- 8.1 The Privacy Officer is responsible for ensuring the Society's compliance with this policy and the *Personal Information Protection Act*.
- 8.2 Stakeholders should direct any complaints, concerns or questions regarding the Society's compliance in writing to the Privacy Officer. If the Privacy Officer is unable to resolve the concern, the stakeholder may also write to the Information and Privacy Commissioner of British Columbia.
- 8.3 Contact information for the Society's Privacy Officer:
- Rebecca Clarke, Executive Director
12138 Fourth Ave. Richmond, BC V7E 3J1
604-664-9192
rebecca.clarke@pc.gc.ca

Approved by Board of Directors: October 8, 2015