

Personal Information Protection
Private Sector Privacy Legislation
Personal Information Protection Policy

Burb Cannabis Corp.
Personal Information Protection Policy

Last updated: February 1, 2022

At Burb Cannabis Corp., we are committed to providing our customers with exceptional service. As providing this service sometimes involves the collection, use and disclosure of some personal information about our customers, protecting their personal information is one of our highest priorities.

While we have always respected our customers' privacy and safeguarded their personal information, we have strengthened our commitment to protecting personal information as a result of British Columbia's *Personal Information Protection Act* (PIPA). PIPA, which came into effect on January 1, 2004, sets out the ground rules for how B.C. businesses and not-for-profit organizations may collect, use and disclose personal information.

We will inform our customers of why and how we collect, use and disclose their personal information, obtain their consent where required, and only handle their personal information in a manner that a reasonable person would consider appropriate in the circumstances.

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

Scope of this Policy

This Personal Information Protection Policy applies to Burb Cannabis Corp.

This policy also applies to any service providers collecting, using or disclosing personal information on behalf of Burb Cannabis Corp.

For our online specific policy for shopburb.com, please refer to: <https://shopburb.com/pages/privacy>

Definitions

Personal Information – means information about an identifiable person. Personal information does not include contact information (described below).

Contact information – means 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.

Privacy Officer – means the individual designated responsibility for ensuring that Burb Cannabis Corp. complies with this policy and PIPA.

Policy 1 – Collecting & Storing Personal Information

- 1.1 Unless the purposes for collecting personal information are obvious and the customer voluntarily provides his or her personal information for those purposes, we will communicate the purposes for which personal information is being collected, either orally or in writing, before or at the time of collection.
- 1.2 We will only collect customer information that is necessary to fulfill the following purposes:
 - To verify identity;
 - To identify customer preferences;
 - To deliver requested products and services
 - To enrol the customer in a program;
 - To ensure a high standard of service to our customers;
- 1.3 We will only collect employee and consultant information that is necessary to fulfill the following purposes:
 - a. Accounting purposes: Payroll, benefits, taxation, invoice reconciliation, etc.;
 - b. Ensure employee certifications, standards and adherence to regulations specific to the cannabis industry and Burb Cannabis Corp.;
 - c. To manage employees administratively (scheduling, time-off, etc.) within the Rise People system whose privacy policy that is acknowledged by all employees, can be found at <https://risepeople.com/privacy-policy/>

1.4 All customer information collected as per section 1.2 of this document is stored within one or a combination of the following secured systems where the data would be protected under the corresponding 3rd party privacy policy. Although each system has opt-out mechanisms, upon request, Burb is able to permanently delete customer data from any or all of these systems.

- a. Shopify - Ecommerce business service - <https://www.shopify.com/legal/privacy>
- b. Klaviyo - Email Service Provider for Marketing purposes - <https://www.klaviyo.com/legal/privacy-notice>
- c. AlpineIQ - Customer Relationship Management / SMS Marketing - <https://alpineiq.com/privacy.html>
- d. Cova - Retail Point of Sale system - <https://www.covasoftware.com/privacy-policy>

1.5 With the exception of information stored in the aforementioned Rise People system (section 1.3), all employee and consultant information collected is stored in a secured and access controlled Google Workspace services environment. No paper copies are maintained.

As per British Columbia cannabis regulations, all employee files are stored for at least 6 years from the date the records were created.

1.6 As required by British Columbia cannabis regulations, video surveillance within the retail floor and secured storage area are recorded and stored on secure on-site physical servers for a period of at least 30 days from time of recording. These recordings are video only with no audio or other biometric or personal information and are provided to LCRB upon request.

Clearly marked signage is posted in areas of surveillance to inform the customers of this practice.

Policy 2 – Consent

- 2.1 We will obtain customer 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 orally or it can be implied where the purpose for collecting, using or disclosing the personal information would be considered obvious and the customer voluntarily provides personal information for that purpose.
- 2.3 Consent may also be implied where a customer is given notice and a reasonable opportunity to opt-out of his or her personal information being used for mail-outs, the marketing of new services or products, and the customer 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), customers can withhold or withdraw their consent for Burb Cannabis Corp. to use their personal information in certain ways. A customer'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 customer in making the decision.

2.5 We may collect, use or disclose personal information without the customer's knowledge or consent in the following limited circumstances:

- When the collection, use or disclosure of personal information is permitted or required by law;
- In an emergency that threatens an individual's life, health, or personal security;
- When the personal information is available from a public source (e.g., a telephone directory);
- When we require legal advice from a lawyer;
- For the purposes of collecting a debt;
- To protect ourselves from fraud;
- To investigate an anticipated breach of an agreement or a contravention of law

Policy 3 – Using and Disclosing Personal Information

3.1 We will only use or disclose customer personal information where necessary to fulfill the purposes identified at the time of collection [*or for a purpose reasonably related to those purposes such as:*

- To conduct customer surveys in order to enhance the provision of our services;
- To contact our customers directly about products and services that may be of interest;]

3.2 We will not use or disclose customer personal information for any additional purpose unless we obtain consent to do so.

3.3 We will not sell customer lists or personal information to other parties [*unless we have consent to do so*].

Policy 4 – Retaining Personal Information

4.1 If we use customer personal information to make a decision that directly affects the customer, we will retain that personal information for at least one year so that the customer has a reasonable opportunity to request access to it.

4.2 Subject to policy 4.1, we will retain customer 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 will make reasonable efforts to ensure that customer personal information is accurate and complete where it may be used to make a decision about the customer or disclosed to another organization.

5.2 Customers 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.

5.3 If the personal information is demonstrated to be inaccurate or incomplete, we will correct the information as required and send the corrected information to any organization to which we disclosed the personal information in the previous year. If the correction is not made, we will note the customers' correction request in the file.

Policy 6 – Securing Personal Information

- 6.1 We are committed to ensuring the security of customer 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 will be followed to ensure that customer personal information is appropriately protected:
The use of user IDs, passwords, encryption, firewalls; restricting employee access to personal information as appropriate (i.e., only those that need to know will have access)
- 6.3 We will use appropriate security measures when destroying customer's personal information such as deleting electronically stored information.
- 6.4 We will continually review and update our security policies and controls as technology changes to ensure ongoing personal information security.

Policy 7 – Providing Customers Access to Personal Information

- 7.1 Customers have a right to access their personal information, subject to limited exceptions.
- 7.2 A request to access personal information must be made in writing and provide sufficient detail to identify the personal information being sought. A request to access personal information should be forwarded to the Privacy Officer.
- 7.3 Upon request, we will also tell customers how we use their personal information and to whom it has been disclosed if applicable.
- 7.4 We will 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.
- 7.5 A minimal fee may be charged for providing access to personal information. Where a fee may apply, we will inform the customer of the cost and request further direction from the customer on whether or not we should proceed with the request.
- 7.6 If a request is refused in full or in part, we will notify the customer in writing, providing the reasons for refusal and the recourse available to the customer.

Policy 8 – Policy for Breach Reporting and Response Process

- 8.1 In case of breach from within Burb organization, Burb follows the below response process:
 - a. A breach should be immediately reported to a Supervisor. Supervisor reports the breach to the Privacy Officer. If the Privacy Officer is unavailable, the Supervisor will assume the role of Privacy Officer for the purposes of managing the breach. The Privacy Officer will immediately report the breach to the 24/7 Breach Reporting Line of BC.
 - b. In consultation with the Breach Reporting Line designated staff, the Privacy Officer will make every effort to stop the breach and recover the information. Further steps might include shut down of the system or equipment, recovering the equipment, change of the codes or correction of the security measures.
 - c. The breach and the measures taken will be documented by the Privacy Officer.
 - d. The affected individuals will be notified of the breach and provided with details such as date and time of the breach, the type of information that leaked, risks to the individual and recommendations of the steps to be taken by the individual to prevent or minimize the potential harm caused by the breach.
 - e. In consultation with the Breach Reporting Line designated staff, the Privacy Officer will review the privacy protection strategies and evaluate the measures. Additional security measures will be applied by Burb if the necessity is determined.

8.2 Burb uses third party vendors to store personal information. In case of a breach notification from the third party supplier, Burb will take the same steps as outlined in 8.1.

8.3 Staff Awareness / Training

Burb's staff is provided with Cyber Security training during the onboarding. The training is concluded with a test and the certificate of completion is provided.

Burb's Managers hold regular conversations with staff to ensure the awareness of the privacy protection standards and requirements in BC, as well as breach response process at Burb.

Policy 9 - Audit Process & Retention

9.1 Quarterly Audit

Burb conducts quarterly audits of the security measures in place to protect personal information. The audits are conducted by the Privacy Officer and a report is submitted to the CFO and the President. As a part of the quarterly audit, the Privacy Officer conducts privacy impact assessment of any new technology or system change. The Privacy Officer reviews administrative, physical and technological safeguards and ensures they are reasonable and effective.

Any findings of ineffectiveness are promptly rectified and suitable safeguards are put into place.

Quarterly audits will take place within 14 days following the end of each quarter - March 31, June 30, September 30 and December 31 of each year.

9.2 Retention

Aforementioned quarterly audits will be stored under access control within our secured Google Workspace virtual server environment and made available for review upon request.

Policy 10 – Questions and Complaints: The Role of the Privacy Officer or designated individual

9.1 The Privacy Officer is responsible for ensuring Burb Cannabis Corp's compliance with this policy and the *Personal Information Protection Act*.

9.2 Customers should direct any complaints, concerns or questions regarding Burb Cannabis Corp' compliance in writing to the Privacy Officer. If the Privacy Officer is unable to resolve the concern, the customer may also write to the Information and Privacy Commissioner of British Columbia.

Contact information for Burb Cannabis Corp's Privacy Officer:

Will Alexander

Head of Marketing / Privacy Officer

Email: will@shopburb.com