BEACON HILL WEALTH MANAGEMENT LTD.

PRIVACY POLICY

EFFECTIVE DATE

APRIL 23, 2026

Table of Contents

PRIVACY POLICY

1. BACKGROUND AND POLICY

The Beacon Hill Wealth Management Ltd. (“Beacon Hill”) privacy policy has been developed to comply with Canada’s *Personal Information Protection and Electronic Documents Act* ("*PIPEDA")* and British Columbia’s *Personal information Protection Act (“PIPA”) (collectively the “Acts”*). PIPEDA and PIPA set out rules for the collection, use and disclosure of personal information in the course of commercial activity as defined in the Acts.

1.1. The Ten Principles of PIPEDA Summarized

The ten principles of PIPEDA that form the basis of this Privacy Policy are as follows:

1. Accountability: organizations are accountable for the personal information they collect, use, retain and disclose in the course of their commercial activities, including, but not limited to, the appointment of a Chief Privacy Officer;

2. Identifying Purposes: organizations are to explain the purposes for which the information is being used at the time of collection and can only be used for those purposes;

3. Consent: organizations must obtain an Individual’s express or implied consent when they collect, use, or disclose the individual’s personal information;

4. Limiting Collection: the collection of personal information must be limited to only the amount and type that is reasonably necessary for the identified purposes;

5. Limiting Use, Disclosure and Retention: personal information must be used for only the identified purposes, and must not be disclosed to third parties unless the Individual consents to the alternative use or disclosure;

6. Accuracy: organizations are required to keep personal information in active files accurate and up-to-date;

7. Safeguards: organizations are to use physical, organizational, and technological safeguards to protect personal information from unauthorized access or disclosure.

8. Openness: organizations must inform their clients and train their employees about their privacy policies and procedures;

9. Individual Access: an individual has a right to access personal information held by an organization and to challenge its accuracy if need be; and

10. Provide Recourse: organizations are to inform clients and employees of how to bring a request for access, or complaint, to the Chief Privacy Officer, and respond promptly to a request or complaint by the individual.

This Privacy Policy applies to Beacon Hill’s Board of Directors, employees and contracted employees. As well, Beacon Hill has third-party service providers sign confidentiality agreements prior to any transfer of an individual’s personal information in the course of providing related information and/or services.

2. DEFINITIONS

"Business 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. Business contact information is not covered by this policy or PIPEDA.

"Chief Privacy Officer" means the individual designated responsibility for ensuring that Beacon Hill complies with this policy and PIPEDA. This person is the CCO who is Dixie Klaibert.

"Data base" means the list of names, addresses and telephone numbers of clients and individuals held by Beacon Hill in the forms of, but not limited to, computer files, paper files, and files on computer hard-drives.

"Express consent" means the individual signs the contract, or other forms containing personal information, authorizing Beacon Hill to collect, use, and disclose the individual's personal information for the purposes set out in the contract.

"Implied Consent" means the organization may assume that the individual consents to the information being used, retained and disclosed for the original purposes, unless notified by the individual.

"Personal Information" means information about an identifiable individual including name, age, home address and phone number, social insurance number, marital status, religion, income, credit history, medical information, education, employment information. Personal information does not include contact information (described below).

"Significant harm" includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.

"Third Party" means a person or company that provides services to Beacon Hill in support of the programs, benefits, and other services offered by Beacon Hill.

3. PURPOSES OF COLLECTING PERSONAL INFORMATION

Unless the purposes for collecting personal information are obvious and the client 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.

We will only collect client, customer, member information that is necessary to fulfill the following purposes:

- To verify identity;
- To verify creditworthiness;
- To identify client preferences;
- To understand the financial needs of our clients;
- To open and manage an account;
- To deliver requested products and services;
- To deliver a high standard of service to our clients; and
- To meet regulatory requirements.

4. CONSENT

We will obtain client consent to collect, use or disclose personal information (except where, as noted below, we are authorized to do so without consent).

Consent can be provided [orally, in writing, electronically, through an authorized representative] or it can be implied where the purpose for collecting using or disclosing the personal information would be considered obvious and the client voluntarily provides personal information for that purpose.

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), clients can withhold or withdraw their consent for Beacon Hill to use their personal information in certain ways. A client's decision to withhold or withdraw their consent to certain uses of personal information may restrict our ability to provide our services. If so, we will explain the situation to assist the client in making the decision.

5. LIMITING COLLECTION

Personal information collected will be limited to the purposes set out in this Privacy Policy, Beacon Hill contracts, and/or other documentation.

Information We Collect: In connection with providing investment products, financial advice, or other services, we obtain non-public personal information about our clients, including:

- Information we receive on account applications, such as address, date of birth, Social Security Number, Social Insurance Number, occupation, financial goals, assets and income;
- Information about transactions with us, our affiliates, or others;
- Information about visits to our website. We store records of the activities on our sites in our web server logs, which automatically capture and save the information electronically. The information we collect helps us administer the site, analyze its usage, protect the website and its content from inappropriate use, and improve the user's experience.
- Information received from credit or service bureaus or other third parties, such as credit history or employment status.

6. LIMITING USE, DISCLOSURE, AND RETENTION

6.1. Use of Personal Information

Personal information will be used for only those purposes to which the individual has consented with the following exceptions, as permitted under PIPEDA:

- the organization has reasonable grounds to believe the information could be useful when investigating a contravention of a federal, provincial or foreign law and the information is used for that investigation;
- an emergency exists that threatens an individual's life, health or security;
- the information is for statistical study or research;
- the information is publicly available;
- the use is clearly in the individual's interest, and consent is not available in a timely way;

- knowledge and consent would compromise the availability or accuracy of the information, and
- collection is required to investigate a breach of an agreement.

6.2. Disclosure and Transfer of Personal Information

Categories of Information We Disclose: We may only disclose information that we collect in accordance with this policy. Beacon Hill Wealth Management does not sell customer lists and will not sell client names to telemarketers.

We will only use or disclose client 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 contact our clients directly about products and services that may be of interest;
- To entities that perform services for us or function on our behalf, including financial service providers, such as a clearing broker-dealer, investment company, or insurance company, other investment advisers;
- To comply with broker-dealer firms that have regulatory requirements to supervise certain representatives' activities;
- To third parties who help manage accounts on our behalf;
- To an attorney, trustee or anyone else who represents a client in a fiduciary capacity;
- To our attorneys, accountants, or auditors; and
- To government entities or other third parties in response to subpoenas or other legal processes as required by law or to comply with regulatory inquiries.

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

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

PIPEDA permits Beacon Hill to disclose personal information to third parties, without an individual's knowledge and consent, to:

- a lawyer representing Beacon Hill;
- collect a debt owed to Beacon Hill by the individual or client;
- comply with a subpoena, a warrant or an order made by a court or other body with appropriate jurisdiction;
- a law enforcement agency in the process of a civil or criminal investigation;
- a government agency or department requesting the information; or
- as required by law.

PIPEDA permits Beacon Hill to transfer personal information to a third party, without the individual's knowledge or consent, if the transfer is simply for processing purposes and the third party only uses the information for the purposes for which it was transferred. Beacon Hill will take measures to provide, by

contractual or other means, that the third party protects the information and uses it only for the purposes for which it was transferred.

6.3. Retention of Personal Information

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

We will retain client, customer, member personal information only as long as necessary to fulfill the identified purposes or a legal or business purpose.

6.4. Data Stored Outside of Canada

Personal information in our possession is stored exclusively in electronic format in our offices in Vancouver, British Columbia, on external secure servers which may result in your personal information being transferred outside of Canada, including to the United States. The laws of other countries regarding the collection, use and disclosure of personal information may be different from the laws of Canada.

For servers located in the United States means data stored on those servers are subject to US laws, including the US Patriot Act (USPA). The USPA gives US government and law enforcement agencies the ability to search data retained by cloud service providers.

6.5 Client's Right to Opt Out

US Federal privacy laws give our clients the right to restrict us from sharing personal financial information. These laws balance your right to privacy with Beacon Hill Wealth Management's need to provide information for normal business purposes. If clients opt out, they limit the extent to which we can provide their personal financial information to non-affiliated companies. Clients have the right to opt out of sharing certain information with affiliated and unaffiliated companies of our firm. Choosing to restrict the sharing of personal financial information will not apply to (1) information shared with non-affiliated service providers that assist us in servicing your account or conducting our business, as permitted by law; and (2) information in response to a court order.

6.6 Closed or Inactive Accounts:

If a client decides to close your account(s) or become an inactive customer, our Privacy Policy will continue to apply.

7. ACCURACY

We will make reasonable efforts to provide that client personal information is accurate and complete where it may be used to make a decision about the client or disclosed to another organization.

Clients may request correction to their personal information for accuracy and completeness clarifications. 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.

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 clients' correction request in the file.

8. SAFEGUARDS

8.1. Use of Safeguards

We are committed to ensuring the security of client personal information in order to protect it from unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks. We restrict access to nonpublic personal information to those individuals who need to know that information to provide products or services and perform their respective duties. We maintain physical, electronic, and procedural security measures to safeguard confidential client information.

The following security measures will be followed so that client personal information is appropriately protected:

- the use of locked filing cabinets;
- physically securing offices where personal information is held;
- 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;
- contractually requiring any service providers to provide comparable security measures; and
- employees and/or Board of Directors are required to sign a confidentiality agreement binding them to maintaining the confidentiality of all personal information to which they have access.

We will use appropriate security measures when destroying client's personal information such as shredding documents and deleting electronically stored information.

We will continually review and update our security policies and controls as technology changes regarding ongoing personal information security.

8.2. Breaches of Security Safeguards

Under PIPEDA, Beacon Hill is required to report to the Office of the Privacy Commissioner ("OPC") and the individual whose information has been breached, any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual. The report is contained herein as Schedule 1.

The individual's notification will be conspicuous and shall contain sufficient information to allow the individual to understand the significance of the breach and any steps they can take to mitigate/reduce harm among other prescribed information. The notification shall be given directly to the individual as soon as feasibly possible.

In determining the real risk of significant harm Beacon Hill will consider:

- the sensitivity of the personal information involved in the breach;
- the probability that the personal information has been, is being or will be misused; and
- any other prescribed factor.

See Schedule 2 for further detail.

If a breach occurs, Beacon Hill will also notify any other organization or government institution of the breach if Beacon Hill believes that the other party may be able to reduce the risk of harm that could result from it.

8.3. Record Keeping of Breaches

Beacon Hill will keep and maintain a record of every breach involving personal information under its control, even if there is no obligation to report or give notice of the breach (i.e. the breach does not create a "real risk of significant harm" to an individual).

The record will contain any information that enables the Commissioner to verify the firm's compliance with the breach reporting and notification obligations. The firm will maintain the record for 24 months after the day on which it determines that the breach has occurred (and may retain same longer to comply with other legal requirements) and will provide the record to the Commissioner on request.

Records must contain any information that enables the OPC to verify compliance with breach of security safeguards reporting and notification requirements in sections 10.1(1) and (3) of PIPEDA, including requirements to assess real risk of significant harm.

Records, at minimum, will include:

- date or estimated date of the breach;
- general description of the circumstances of the breach;
- nature of information involved in the breach;
- whether or not the breach was reported to the Privacy Commissioner of Canada/individuals were notified; and
- sufficient details for the OPC to assess whether the firm has correctly applied the real risk of significant harm standard and otherwise met its obligations to report and notify in respect of breaches that pose a real risk of significant harm

9. OPENNESS

Beacon Hill will endeavour to make its privacy policies and procedures known to the individual via this Privacy Policy as well as the firm's *Privacy Statement*, contained herein as Schedule 3.

10. INDIVIDUAL ACCESS

Clients have a right to access their personal information, subject to limited exceptions. Exceptions to access that might apply include:

- information that is prohibitively costly to provide;
- information that contains references to other individuals;
- information that cannot be disclosed for legal, security, or commercial proprietary reasons, and
- information that is subject to solicitor-client or litigation privilege.

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 Chief Privacy Officer.

Upon request, we will also tell clients how we use their personal information and to whom it has been disclosed if applicable.

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.

A minimal fee may be charged for providing access to personal information. Where a fee may apply, we will inform the client of the cost and request further direction from the client on whether or not we should proceed with the request.

If a request is refused in full or in part, we will notify the client in writing, providing the reasons for refusal and the recourse available to the client.

11. COMPLAINTS/RECOURSE

If an individual has a concern about Beacon Hill's personal information handling practices, a complaint, in writing, may be directed to the Chief Privacy Officer.

Upon verification of the individual's identity, the Chief Privacy Officer will act promptly to investigate the complaint and provide a written report of the investigation's findings to the individual.

Where the Chief Privacy Officer makes a determination that the individual's complaint is well founded, the Chief Privacy Officer will take the necessary steps to correct the offending information handling practice and/or revise Beacon Hill's privacy policies and procedures.

Where the Chief Privacy Officer determines that the individual's complaint is not well founded, the individual will be notified in writing.

If the individual is dissatisfied with the finding and corresponding action taken by Beacon Hill's Chief Privacy Officer, the individual may bring a complaint to the Office of the Privacy Commissioner.

PRIVACY STATEMENT SUMMARY

PRIVACY STATEMENT

PURPOSE

Protecting our clients' privacy is a priority for Beacon Hill Wealth Management Ltd. ('Beacon Hill'). These Privacy Principles are adhered to by Beacon Hill to ensure that the information submitted to us will be treated with the utmost confidentiality and in compliance with the *Personal Information Protection and Electronic Documents Act of Canada* (PIPEDA) and the *Personal information Protection Act* (PIPA) of British Columbia.

PRINCIPLES

Accountability

We are responsible for all personal information under our control and have designated a Privacy Officer who is accountable for our compliance with these following principles. The Privacy Officer is Dixie Klaibert.

Identifying Purposes

We will identify and document the purposes for which we collect, use or disclose personal information at or before the time the information is collected.

Consent

The knowledge and consent of our clients are required for the collection, use or disclosure of personal information.

Limiting Collection

Only such information as is necessary for Beacon Hill's services will be collected from our clients. When personal information is needed, it will be obtained directly from our clients.

Limiting Use, Disclosure and Retention

Personal information will not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by the law. Personal information will be retained only as long as necessary for fulfilment of those purposes.

Accuracy

Personal information will be as accurate, complete and up-to-date as necessary for the purposes for which it is to be used.

Safeguards

We will protect personal information with security safeguards appropriate to the sensitivity of our client's personal information.

Openness

Beacon Hill will make available to client's specific information concerning the policies and procedures relating to the management of their personal information.

Individual Access

Upon your request, you will be informed of the existence, use and disclosure of your personal information and shall be given access to that information. You may verify the accuracy and completeness of the information and may request that it be amended, if appropriate.

Handling Client Complaints and Suggestions

Any question, concern or complaint about any of these principles can be addressed to our Privacy Officer at admin@beaconhillwm.ca or phone at 778-433-1314. A complete version of Beacon Hill's Privacy Policy is available upon request.