

# Privacy Policy

## DOCUMENT INFORMATION

<b>EFFECTIVE DATE</b>	June 18, 2024
<b>LAST MODIFIED DATE</b>	June 18, 2024
<b>NEXT REVIEW DATE</b>	June 2026
<b>CURRENT VERSION</b>	1.0
<b>DOCUMENT OWNER</b>	Senior Vice President, Finance and Operations
<b>DOCUMENT AUTHOR</b>	Senior Vice President, Finance and Operations
<b>APPLIES TO</b>	All Foundation Staff

## PURPOSE

VGH & UBC Hospital Foundation (the "Foundation") respects and commits to the protection of the privacy and confidentiality of all information entrusted to the foundation. Therefore, the Foundation has established this Privacy Policy to comply with applicable municipal, provincial, and federal privacy legislation.

Respect for the organization's privacy and confidentiality is of utmost importance.

The Foundation strives to comply with the British Columbia private-sector privacy legislation, the *Personal Information Protection Act*, SBC 2003, c. 63 ("PIPA"). The Privacy Policy, together with any associated data protection documentation that flows from this Policy, aims to comply with PIPA.

### Confidential Information

The following is considered confidential information:

- All matters/documentation relating to existing donors or potential donors
- All contracts.
- All Human Resources files and proceedings.
- All financial information, status and statements.
- All information or documentation labelled "Confidential" by the foundation, or listed as such by separate memorandum, or e-mail that advises confidential status.

This information may be related to, without being limited to, personal information of any kind about donors or employees, volunteers, contractors as well as information about the operations of the Foundation (e.g., personnel matters, internal financial procedures, contractual information, and intellectual property of the Foundation).

Confidential information shall not be used for any purpose other than its reasonable use in the normal performance of employment duties.

## Personal Information

“Personal Information” has the meaning assigned to it under s. 4 of PIPA, namely any information “about an identifiable individual, and includes employee personal information, but does not include contact information or work product information.”

The Foundation collects, uses, and shares Personal Information about our donors, employees, and volunteers in order to:

- Contact individuals about our fundraising activities.
- Contact donors and stakeholders to evaluate our foundation’s work.
- Conduct research or lead generation.
- Employ or participate in the work of the foundation.

All access to Personal Information must be justified by compelling circumstances required by staff to perform their duties. Therefore, access thereto is provided only on a pure “need-to-know” basis. “Staff” includes internal Foundation employees, volunteers, third-party contractors and service providers, and their employees.

If a Foundation staff member commits a privacy breach by accessing, using, disclosing, or retaining personal information for purposes other than in the performance of their duties, they may be subject to discipline, including possible suspension or termination of employment (subject to any exceptions under employment standards laws and regulations).

## SCOPE

This Privacy Policy governs the access and use of Personal Information by employees, volunteers, and contractors within the Foundation. For certainty, “staff” refers to both internal Foundation employees and to contractor employees who are external to the Foundation.

## DONOR PRIVACY

The Foundation is committed to protecting privacy by ensuring that:

- The Personal Information it receives is kept safe, secure, confidential, accurate, and up-to-date;
- Donors understand why their Personal Information is collected by the Foundation;
- The Foundation provides notice prior to the collection, use, disclosure, and storage of donor Personal Information;
- The Foundation obtains donor consent (as appropriate) before collecting, using, sharing or releasing donor information, except as set out in this policy or permitted or required by law;
- The Foundation collects only the Personal Information necessary to carry out services and to fulfill the mandate of the Foundation, unless otherwise consented to by the donor;
- access to donor information is limited to the Foundation's employees and volunteers, involved in delivering services to donors;
- any external agents to whom the Foundation releases or discloses Personal Information must have a need to know or receive that information, and these agents shall only use and disclose donor or other Personal Information for the purpose(s) for which it was originally provided;
- donors can withdraw their consent at any time to the collection, use, disclosure, and storage of their Personal Information;
- donors have access to their own personal records, except where the Foundation is entitled to refuse part or all of an access request as per applicable law;
- donors are able to copy or correct their record and ask questions about the Foundation's privacy policies and procedures;
- complaints about the Foundation's privacy policies and procedures are to be handled efficiently and effectively by the Foundation's Privacy Officer;
- establishing parameters for instances where the Foundation collects Personal Information *indirectly* (i.e. if it originates from persons or sources who are not the people to whom the Personal Information pertains), as long as it aligns with PIPA;
- providing notification and / or obtaining consent from persons at the moment that the Foundation starts collecting Personal Information beyond the confines of situations where implied consent may be relied upon to collect data; and
- ensuring that all legal and regulatory requirements regarding donor information are met and maintained.

## RESPONSIBILITIES

### Appointment of Privacy Officer

The Privacy Officer for the Foundation is the Senior Vice President, Finance and Operations. The Privacy Officer is responsible for all donor-related privacy inquiries and complaints. The Privacy Officer has the authority to delegate their duties on an "as needed" basis.

The contact information for the Privacy Officer is available on the Foundation website.

The duties of the Privacy Officer include:

- maintaining ongoing knowledge of privacy legislation and regulations, and any developments in those laws that may affect the Foundation;
- ensuring that all employees and volunteers have training and re-training (as required) on the Foundation's privacy policy and practices;
- monitoring employee compliance with the Foundation's privacy policy;
- responding to privacy-related complaints and concerns;
- responding to requests for access and correction;
- responding to inquiries from the public about the Foundation's privacy practices;
- liaising with other organizations, the public and government, as necessary, on privacy-related issues; and
- acting as the single point of contact in the event of a privacy audit or investigation instigated by the Office of the Information & Privacy Commissioner of B.C., or any other privacy regulator with the jurisdiction to investigate the Foundation's privacy program or activities.

### **Managers (Leadership Team, Directors, and Managers)**

Managers are responsible for the day-to-day collection, use, and safeguarding of Personal Information under their control. They shall ensure that employees and any volunteers with access to Personal Information, are aware of and receive training on privacy procedures and practices established by the Foundation for the collection, use, disclosure and safeguarding of Personal Information.

Managers must adhere to their obligations under Privacy Breach Management Protocol, which outlines requirements and steps to follow on discovering or being notified of a suspected privacy incident or breach.

### **Staff**

All Staff who have access to Personal Information or confidential Information are responsible for complying with this Policy and with PIPA. Staff are required to:

- Complete privacy training when on-boarded into the Foundation, and to comply with any privacy re-training as imposed or recommended by the Privacy Officer;
- ensure that access to and disclosure of Personal Information or Confidential Information is only made by or to authorized individuals;
- ensure that reasonable measures are taken to prevent any unauthorized access, disclosure, loss or theft of information;
- comply with terms of use and security requirements for electronic systems; and
- report to the Privacy Officer any actual or suspected breaches of privacy or this policy and cooperate with the Senior Leadership and Human Resources for the purposes of any investigation.

## **CONFIDENTIALITY AND PRIVACY AGREEMENT**

All Foundation staff and volunteers will sign an agreement that outlines their obligations to abide by confidentiality and privacy rules as part of their initial hiring or orientation. The signed Agreement will be placed in the employee or volunteer file. They will not have access to any confidential information until after they have signed the Agreement.

Any breach of confidentiality whether real or suspected should be reported as follows:

- if related to donors, the breach should be reported to the relevant Manager who will involve the Foundation Privacy Officer
- if related to employees, the breach should be reported to the relevant Manager who will involve the Vice President, People and Organizational Effectiveness
- if related to financial matters, the breach should be reported to the relevant Manager who will involve the Senior Vice President, Finance and Operations.

## **ACCESS TO PERSONAL INFORMATION**

To safeguard privacy, the Foundation shall treat Personal Information according to these principles:

- Personal Information is to be disclosed to staff and other stakeholders on a pure “need-to-know” basis.
- Personal Information is to be used, disclosed, and stored only if doing so is consistent with the original purpose for which the Personal Information was collected.
- Any secondary use of Personal Information – that is, any use of Personal Information that differs substantively from the original purpose for its collection – requires express written consent from the person(s) to whom the Personal Information pertains.
- Internal access to any Personal Information is assigned based on the role of the staff member and their need to access Personal Information.

The principle of “least privilege” governs. This means that only the minimum amount of Personal Information required to perform a task shall be granted at all times.

## **PRIVACY BREACH REPORTING**

Privacy is everyone’s responsibility at the Foundation. Although the Privacy Officer is responsible for addressing privacy related concerns and investigating any issues, all staff (including contractors) are obliged to report any privacy breaches as soon as they are identified.

To report a privacy breach, contact the Privacy Officer. The Privacy Officer shall thereafter file a report and investigate further.

When reporting a privacy breach, please provide as much information as possible. This includes the date and time of the suspected breach, the Personal Information involved, any person(s) involved, and any additional details. The staff member reporting the breach must cooperate with the Privacy Officer and any other person(s) tasked with investigating the breach. Any refusal to cooperate may result in

disciplinary action, and more serious consequences if the staff member attempts to “cover up” salient details or interfere with the investigation.

## **PRIVACY IMPACT ASSESSMENTS**

A Privacy Impact Assessment (“PIA”) may be completed before implementing or significantly changing any program or system that requires the collection, use, disclosure or sharing of Personal Information.

Before undertaking any new initiative, program or activity that involves Personal Information, Foundation departments must contact the Privacy Officer to determine whether a PIA is required. Completion of a PIA is the responsibility of the department undertaking the program or activity, with support from the Privacy Officer.

Similarly, the Privacy Officer may also direct that a PIA be retroactively conducted on any legacy systems, programs, contracts, or other arrangements that involve Personal Information if no such due diligence activity had previously taken place.

## **SAFEGUARDING OF PERSONAL INFORMATION**

- Donor information stored electronically is protected by encryption, password, and other technical security measures. Access to the foundation’s electronic database is limited on a need-to-know basis for added security.
- Donor information collected in hard copy form is stored in locked cabinets accessible only by the foundation’s employees, students, and volunteers.
- Access to donor information will be limited to those who need to know the information for the purposes set out in the donor’s consent or as otherwise permitted or required by law.
- The Foundation’s employees will never leave donor Personal Information, in paper or electronic form, unattended or exposed to anyone other than the donor.
- The foundation will not send Confidential Information or Personal Information to donors by email without the donor’s prior consent. Personal Information sent to donors will be done so via secure email (Note that secure email ensures messages are encrypted). If donors state they do not wish to receive emails in a secure method, the Foundation staff shall inform donors that the foundation does not accept responsibility for communications sent in a non-secure way.
- Donor information transmitted via email to third parties shall be sent in an encrypted format.
- Communication between staff within the vghfoundation.ca domain is secure in transmission.
- The Foundation requires external agents, such as third-party auditors, to maintain the confidentiality of donor information and to refrain from using donor information for any purpose other than the purposes for which consent was provided by the donor. Where appropriate and necessary, the Foundation will obtain the consent of the donor to disclosure of information to external agents. (External agents are persons or companies with which the Foundation has contracts and that may come into contact with personal information.)
- When disposal is permitted or required, records of donor personal information will be disposed of in a secure manner such that reconstruction of the records is not reasonably foreseeable in the circumstances.

## **CONSENT FOR RECORDING, PHOTOGRAPHING AND/OR FILMING**

Employees, volunteers, as well as all donors and members of the public will be asked to provide their informed and/or written consent prior to any recording, photographing, or filming that may be used for promotional, educational, or training purposes by the foundation. Requests for participation in media-conducted interviews or other activities for publication in print, online and/or for broadcasting purposes will be co-ordinated through the Marketing and Brand Engagement department with specific waivers provided by the media organization.

## **THE FOUNDATION PROPERTY**

Upon termination of employment with the Foundation, employees shall promptly return (without duplicating or summarizing), any and all material pertaining to the Foundation business in their possession including, but not limited to: all donor information (charts, lists, databases, etc.), physical property, documents, keys, electronic information storage media, manuals, letters, notes and reports.

## **EDUCATION & TRAINING**

All Foundation staff, including employees and contractors, are required to undergo privacy protection training. The Foundation will ensure that Staff who manage, access, or use Personal Information receive privacy and information management training when initially hired and as required on an ongoing basis. The Foundation will develop privacy education programs to educate all Staff and users of Personal Information about the Foundation's privacy obligations under PIPA. Annual re-training must be completed by all staff, and re-training must be delivered in the event of a major privacy breach, or security incident where Personal Information is involved.

Proof of privacy education, training, and re-training may be requested by the OIPC or other external auditor to evidence ongoing due diligence measures taken by Foundation.

The Foundation will use its best efforts to keep confidential the name and identifying, information of any Staff who report an actual or suspected breach of privacy or violations of this Policy.

## **CHANGES TO PRIVACY POLICY**

The Foundation reserves the right to modify, change, or update this Internal Privacy Policy from time to time. Specifically, modifications may be made in the following circumstances:

- In the event of any changes to the way Foundation collects, uses, discloses, and retains Personal Information;
- If there are substantive changes in applicable legislation that affects the way Foundation processes Personal Information; or
- If Foundation conducts a regular revision of this Policy in order to clarify language as part of ordinary due diligence and compliance activities.

## **PROCEDURAL DOCUMENTS**

Access, use, disclosure, and retention of Personal Information within the Foundation is governed by this Privacy Policy and any standard operating procedures or other similar documents. The Foundation may create operational or procedural documents using the principles of privacy protection outlined in this Privacy Policy.

## **FURTHER INFORMATION**

If you have any questions or concerns regarding this Privacy Policy, or if you have any queries relating to the collection, use, disclosure, and storage of your Personal Information, contact the Foundation Privacy Office.

Additionally, you also contact the Foundation Privacy Officer in writing if you wish to obtain a copy of the Personal Information has collected about you.

For general questions about privacy laws and regulations, you may contact the Office of Information & Privacy Commissioner of British Columbia at <https://www.oipc.bc.ca/>.



**APPENDIX**

**Data Map**

The charts below are non-exhaustive lists of Personal Information that Foundation collects. From time to time, the scope of PI may expand depending upon the necessity of collecting that Personal Information.

Foundation retains a copy of the Personal Information collected in a data map, which will be continuously updated to maintain accuracy. This is particularly critical if or when the scope of Personal Information processed by the organization changes.

**PERSONAL INFORMATION – DONORS**

In addition to the above, the following PI is collected from donors to the Foundation:

Name	Home Address	Personal Phone Numbers (s)
Credit / Debit Card Number	Donation History	Net Work / Income
Properties / Real Estate Holdings	Third Party Beneficiary Information	Shareholdings (Corporate Registry)
Wills	Billing / Shipping Address	

**PERSONAL INFORMATION – EMPLOYEES**

In addition to the above, the following PI is collected from Foundation staff:

Employment Start Date	Employment End Date	Performance Reviews
Credit Check	Wage Rate / Salary	Social Insurance Number
Banking Information (for direct deposit of salaries and wages)	Tax Information (CRA Compliance and Tax Filing Purposes)	Religious Beliefs (to accommodate religious holidays)
Health Information (for health benefits)	Third-Party Contact Information (Emergency)	Employee Device Use (on corporate-owned assets)
Citizenship / Work Permit Status	Dietary Restrictions	Image / Likeness
Indigenous Status	Resume / CV	
Marital Status	Benefits / Compensation	Background Check Result

**PERSONAL INFORMATION – VOLUNTEERS**

In addition to the above, the following PI is collected from volunteers:

Name	Address	Email Address
Phone Number	Third-Party Contact Information (Emergency)	Headshot
Confidentiality agreement	Parental consent (for underage volunteers)	Bio

## PERSONAL INFORMATION – BOARD MEMBERS

In addition to the above, the following PI is collected from board members:

Name	Address	Email Address
Phone Number	Meetings / Board Activities	
Bio	Headshot	Business sector/role/background
Conflict of interest disclosure	Confidentiality agreement	Gender / Gender Identity (Optional)
Spousal information	Date of Birth / DOB (Optional)	Religious Beliefs (Optional)
Disability Status (if required for accommodation)	Education (optional)	
Ethnicity / Race (Optional)	Nationality / Citizenship (Optional)	

## PERSONAL INFORMATION – LEADS

In addition to the above, the following PI is collected from leads and potential donors to the Foundation. This information may only be collected from publicly available sources or government services, unless the donor provides the information directly to the Foundation:

Name	Business Address	Business Contact Information
Real Estate Holdings	Patient Linkage / Medical History	Shareholdings (Corporate Registry)
Education History	Corporate Leadership History	Net Worth / Income
Awards & Honours	Affinity / Volunteerism	Family Life
Donation History	Social Media Links	Age / Date of Birth
Likeness / Image		

## VERSION HISTORY

VERSION	DESCRIPTION OF CHANGE	APPROVED BY	APPROVAL DATE
1.0	First version.	Board of Directors	June 18, 2024