THE IRVING K. BARBER
British Columbia Scholarship Society
ADMINISTERED BY THE VICTORIA FOUNDATION

The Irving K. Barber British Columbia Scholarship Society

POLICES RELATING TO PRIVACY AND THE PROTECTION OF PERSONAL INFORMATION

This document contains the following sections:

For information on any of the contents of this document, please contact the Society's Privacy Officer:

Privacy Officer,
Irving K Barber British Columbia Scholarship Society
109-645 Fort Street
Victoria, BC V8W 1G2

phone: (250) 381-5532 or e-mail: info@BCScholarship.ca

Updated: January 2009

PERSONAL INFORMATION PROTECTION POLICY

The Irving K. Barber British Columbia Scholarship Society is committed to providing our educational community with exceptional service. As providing this service involves the collection, use and disclosure of some personal information about our student applicants, protecting their personal information is one of our highest priorities.

While we have great natural respect for all persons' privacy, 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. not-for-profit organizations may collect, use and disclose personal information.

We will inform all of our student applicants 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 student applicant personal information. Our privacy commitment includes ensuring the accuracy, confidentiality, and security of our student applicant personal information and allowing our student applicants to request access to, and correction of, their personal information.

Scope of this Policy

This Personal Information Protection Policy applies to the Irving K. Barber British Columbia Scholarship Society and its Agents, Committees and Sub-committees and to any individuals or organizations collecting, using or disclosing Personal Information on behalf of the Irving K. Barber British Columbia Scholarship Society (collectively, the "**Society**").

Definitions

Personal Information – means information about an identifiable *individual (e.g., name, age, home address and phone number, social insurance number, marital status, religion, income, credit history, medical information, education, employment information).*

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

Policy 1 – Collecting Personal Information

1.1 Unless the purposes for collecting Personal Information are obvious and the student applicant 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 Personal Information that is necessary to fulfill the following purposes:

- To verify identity and confirm the accuracy and completeness of student applications;
- To process the student application for consideration of an award;
- To facilitate the adjudication process;
- To send out information to, or communicate with, student applicants;
- To ensure a high standard of service to our student applicants;
- To meet regulatory requirements;
- To award scholarship funds and issue tax forms;
- Where appropriate, to communicate the names and relevant accomplishments of award recipients;
- To conduct relevant research.

Policy 2 – Consent

2.1 We will obtain the student applicant's 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 in writing or it can be implied where the purpose for collecting using or disclosing the Personal Information would be considered obvious and the student applicant voluntarily provides Personal Information for that purpose.

2.3 Subject to certain exceptions (*e.g. the Personal Information is necessary to provide the service or the withdrawal of consent would frustrate the performance of a legal obligation),* the student applicant can withhold or withdraw their consent for the Society to use their Personal Information in certain ways. A student applicant's decision to withhold or withdraw their consent to certain uses of Personal Information may restrict our ability to consider provision of a scholarship award. If so, we will explain the situation to assist the student applicant in making the decision.

2.5 We may collect, use or disclose Personal Information without the student applicant's knowledge or consent in the following limited circumstances:

A full listing of such circumstances can be found in sections 12, 15, and 18 of PIPA. Some examples include:

- 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;
- To protect ourselves from fraud; or
- 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 a student applicant's Personal Information where necessary to fulfill the purposes identified at the time of collection.

3.2 We will not use or disclose a student applicant's Personal Information for any additional purpose unless we obtain consent to do so.

3.3 We will not sell student applicant lists or Personal Information to other parties.

Policy 4 – Retaining Personal Information

4.1 If we use a student applicant's Personal Information to make a decision that directly affects the student applicant, we will retain that Personal Information for at least one year so that the student applicant has a reasonable opportunity to request access to it.

4.2 Should the student applicant be the recipient of any financial award, the student Personal Information will be retained for any period required by law.

4.3 Subject to the other provisions of Policy 4, we will retain student applicant's 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 student applicant's Personal Information is accurate and complete where it may be used to make a decision about the student applicant or disclosed to another organization.

5.2 Student applicants may request correction of 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 student applicant's correction request in the file.

Policy 6 – Securing Personal Information

6.1 We are committed to ensuring the security of all student applicant Personal Information in order to protect it from unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks.

6.2 The following security measures will be followed to ensure that student applicant Personal Information is appropriately protected:

Examples may include: the use of locked filing cabinets; physically securing offices where Personal Information is held; the use of user IDs, passwords, encryption, firewalls; and restricted 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 student applicant Personal Information such as securely shredding documents and 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 – Governance of Records

7.1 The Society shall retain proper custody, care and control over any and all records received by, or authored and generated any member of the Society, that contain Personal Information.

7.2 All individuals associated with the Society who are in possession of or who have access to Personal Information must provide all reasonable security protection and safe storage for the Personal Information in their possession or under their control.

7.3 All individuals associated with the Society who are in possession of or who have access to Personal Information must not use or disclose any Personal Information for any purposes other than those authorized by the Society and these shall be limited to the purposes for which consent has been obtained.

7.4 All individuals associated with the Society shall make available to the Chair of the Society Board, and to the Privacy Officer, any and all records containing Personal Information that may be in the their custody, care or control, at any time and upon request for the purposes of audit, inspection, or to facilitate the duties of the Privacy Officer.

7.5 All records containing Personal Information that are in the custody, care or control of any individuals associated with the Society shall revert into the care, custody and control of the Society once the individuals no longer require the records to complete the tasks for which they were provided with those records. The Society shall assume full responsibility for the safe storage and security of these records after they revert to the care, custody and control of the Society.

7.6 The Society shall retain records in its care, custody and control only for the time required by law, at which time a motion shall be brought before a meeting of the Board recommending either a period of further retention, with explanation, or the destruction of those records by securely shredding documents and/or permanently deleting electronically stored information.

7.7 The person appointed as the Secretary of the Society Board, and any persons appointed as Committee Secretary by any Committee Chairs, shall be the persons responsible for the functional care, custody and control of all records containing Personal Information. The satisfactory execution of this duty by the appointed Secretaries will be the supervisory responsibility of the Chairperson to whom they report.

Policy 8 – Providing Student Access to Personal Information

8.1 Student applicants have a right to access their Personal Information, subject to limited exceptions. A full listing of the exceptions to access can be found in section 23 of PIPA. Some examples include: solicitor-client privilege, or when disclosure would reveal Personal Information about another individual.

8.2 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 Society's Privacy Officer.

8.3 Upon request, we will also tell student applicants how we use their Personal Information and to whom it has been disclosed, if applicable.

8.4 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.

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

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

Policy 9 – The Authority of the Privacy Officer

9.1 The Privacy Officer is responsible for ensuring the Society's compliance with this policy and PIPA.

9.2 The Privacy Officer is responsible for all duties and responsibilities outlined and required under PIPA, and shall deliver those duties and responsibilities under the direction, and at the discretion, of the Chair of the Society Board.

9.3 The Privacy Officer shall be responsible for the provision, maintenance and updating of this Personal Information Protection Policy, in keeping with PIPA, to be ratified by the Board as required. The Privacy Officer will be responsible for the distribution of the Personal Information Protection Policy to all members of the Society and, on request, to any members of the public as appropriate.

9.4 The Privacy Officer shall be authorized and required to act in accordance with all provisions of the Personal Information Protection Policy, including following the Breach of Privacy Protocol in the event that a privacy breach occurs.

9.5 For the purposes of executing the duties and responsibilities required under PIPA, the Privacy Officer shall have unrestricted access to any and all records extant throughout the Society and its committees and shall have the full cooperation of all appointed Secretaries as may be required to access and identify such records.

9.6 The Privacy Officer shall conduct an annual privacy audit, at the Privacy Officer's discretion or as may be directed by the Chair of the Society Board. This audit will review the safe storage and security of Society's records and the Society's adherence to its Personal Information Protection Policy.

9.7 The Privacy Officer shall submit the privacy audit to the Society Board at its annual general meeting, describing the findings of the annual audit, along with any recommendations or advice.

Policy 10 – Questions and Complaints

The Role of the Society's Privacy Officer

10.1 As a first step, student applicants should direct any complaints, concerns or questions regarding the Society's compliance to the Privacy Officer in writing. If the Privacy Officer is unable to resolve the concern, the student applicant may also write to the Information and Privacy Commissioner of British Columbia.

Contact information for the Privacy Officer:

Privacy Officer, Irving K Barber British Columbia Scholarship Society
109-645 Fort Street, Victoria, BC V8W 1G2
phone: (250) 381-5532 or e-mail: info@BCScholarship.ca

The Role of the Privacy Commissioner

10.2 Under PIPA, the Office of the Information and Privacy Commissioner (OIPC) may be asked to review matters where an individual is not satisfied with how an organization has responded to a request for personal information, a request for correction of personal information, a complaint about how it treats personal information or if the organization does not follow any provision of PIPA.

In order to request a review or make a complaint, send a written request to the OIPC (if you are requesting a review, you must do so within 30 working days of receiving a response from the Society). Include all correspondence between you and the Society, as well as any other relevant information (such as dates, names and details of conversations you have had with individuals within the Society). **Please note that the OIPC does not accept requests for review or complaints via e-mail.**

Although PIPA does not impose a time limit for making a complaint, a complaint or request for review to the OIPC should be made at the earliest opportunity. Unless there are extenuating reasons, the OIPC will not generally allow a complaint made more than 6 months after the individual concerned had notice of the circumstances.

Contact information for the Privacy Commissioner:

Office of the Information and Privacy Commissioner for British Columbia
PO Box 9038, Stn. Prov. Govt., Victoria, BC V8W 9A4
phone: (250) 387-5629 or e-mail: info@oipc.bc.ca; website: www.oipc.bc.ca

Breach of Privacy Protocol

A breach of privacy is a serious matter. Once the Society's Privacy Officer learns that a possible personal privacy breach has occurred, immediate action will be taken. The following protocol will assist the Society in controlling the situation by ensuring that the following steps will be taken. Many steps will have to be delegated so that they may be carried out simultaneously or in quick succession.

STEP 1. IDENTIFY: Identify the nature and scope of the alleged breach and take initial steps to catalogue the records and information compromised. Containing the initial damage may involve the following:

- determining whether the privacy breach would allow unauthorized access to an electronic information system
- notifying any effected systems security staff
- shutting down a system
- securing a crime scene until police arrive

STEP 2. REPORT: Ensure that appropriate Board members are immediately notified of the breach, including the Chairperson of any effected sub-committees This report should indicate:

- whose personal information was disclosed
- to whom it was disclosed
- when it was disclosed
- how it was disclosed/accessed
- what steps have been taken in response to the disclosure

STEP 3. RETRIEVE: Any documents that have been disclosed to, or taken by, an unauthorized recipient should, if possible, immediately be retrieved or destroyed (especially in cases where information has been sent by fax or electronic mail). This will require personal attention by the Privacy Officer to secure the documents and return them to their original location or send them to the intended authorized recipient. Retrieving records may also require the assistance of IT Systems Security staff.

STEP 4. INFORM: In cases where the breach may result in consequences that would directly affect the person whose information has been disclosed, that person should be informed of the details of the breach. They should also be informed of the Society's efforts to retrieve this information and prevent a similar breach from reoccurring. If affected parties are notified of the breach by letter, the letter should be reviewed by the Chairperson of the Board prior to being sent. Should this breach be identified as a result of a complaint then efforts should be made to resolve the complainant's concerns informally, at the onset of the complaint.

STEP 5. DAMAGE CONTROL: The Society's Privacy Officer will work with the Board to assist in deciding how best to communicate the privacy breach to affected third parties and, if necessary, provide a news release.

STEP 6. INVESTIGATE: The Society's Privacy Officer will investigate the details of any breach, for the purpose of determining and recording all the relevant facts concerning the breach and making recommendations. The objectives of this investigation should include: a review of the circumstances surrounding the event as well as the adequacy of existing policies and procedures in protecting personal information.

STEP 7. BOARD REVIEW/DE-BRIEFING: The Society Privacy Officer will report the details of the breach of privacy and remedial steps to the Board of Directors and all Committee Chairs. The Board may direct the Society as a whole to review and implement the report's recommendations.

Part of this review may include:

- Conducting a Privacy Impact Assessment on a system or program to ensure compliance with the collection, use, disclosure, security and storage provisions of the *Personal Information Protection Act.*
- A Security Threat and Risk Assessment.
- A debriefing session with any Board members or staff to identify what was learned from the breach and what could be done to prevent a similar situation

STEP 8. OFFICE of the INFORMATION AND PRIVACY COMMISSIONER: At the Board's direction, the Society's Privacy Officer will report the breach of privacy and the remedial action taken to the Office of the Information and Privacy Commissioner.