

HAZLITT STEEVES HARRIS LLP

CHARTERED ACCOUNTANTS

PRIVACY STATEMENT

Introduction

Hazlitt Steeves Harris LLP Chartered Accountants collects, uses and discloses personal information in the possession, or under the control, of its clients to the extent required to fulfill its professional responsibilities and operate its business. The firm is committed to maintaining the privacy of personal information provided by its clients and protecting all personal information in its possession or control. This Privacy Policy sets out the principles and procedures that the firm follows in meeting its privacy commitments to its clients and complying with the requirements of federal and provincial privacy legislation.

Principle #1: The firm is accountable for personal information in its possession or control.

- The firm is accountable for all personal information in its possession or control. This includes any personal information that the firm received directly from clients who are individuals, or indirectly, through clients that are organizations (e.g., corporations, government entities, not-for-profit organizations).
- The firm has:
 - established and put into effect policies and procedures aimed at properly protecting personal information;
 - educated its partners and employees regarding its privacy policy and their role and responsibilities in keeping personal information private; and
 - appointed its Chief Privacy Officer to oversee privacy issues at the firm.
- If you have any questions about the firm's privacy policies and practices, the firm's Privacy Officer can be reached by email at rdunn@hshca.com, by phone at (519) 336-6133 and by letter at 301 North Front Street, Sarnia, ON, N7T 5S6.

Principle #2: The firm identifies the purposes for which it collects personal information from clients before it is collected.

- The firm collects personal information from clients and uses and discloses such information only to provide the professional services that the client has requested. The types of information that may be collected for this engagement, and the purposes for which it is collected, are set out under Principles 3 and 4 of this privacy statement.

Principle #3: The firm obtains a client's consent before collecting personal information from that client.

- The engagement letter to which this privacy statement is attached sets out your responsibility to obtain any consents required under applicable privacy legislation for collection, use and disclosure to us of personal information. By signing the engagement letter, you are formally acknowledging this responsibility.

Such personal information could include:

- *home addresses*
- *home telephone numbers*
- *personal identification numbers (e.g., social insurance numbers, credit card numbers)*
- *financial information (credit ratings, payroll information, personal indebtedness)*
- *personnel information (e.g., employment history, references to criminal records)*
- *information linked to the type of client, for example:*
 - *information in medical records (with respect to organizations such as hospitals or medical practices)*
 - *information related to race, religion, sexual preference, receipt of welfare or subsidized housing (with respect to various types of not-for-profit and government entities)*
 - *source data in claims and in-force databases (with respect to insurance companies)*
 - *tenant information (with respect to residential leasing companies).*

Principle #4: The firm collects only that personal information required to perform its professional services and operate its business and such information is collected by fair and lawful means.

The partners and staff involved in this engagement may need access to some or all of the types of personal information, noted under principle 3 above, to obtain evidence to support the firm's opinion on the company's financial statements and the preparation of the company's corporation income tax returns. Such personal information may be a significant component of various transactions and events affecting the financial statements that will be subjected to confirmation, testing, analysis and such other procedures as the firm considers necessary to perform an audit in accordance with generally accepted auditing standards.

Principle #5: The firm uses or discloses personal information only for purposes for which it has consent, or as required by law. The firm retains personal information only as long as necessary to fulfill those purposes.

- As required by professional standards, rules of professional conduct and regulation, the firm documents the work it performs in records, commonly called working paper files. Such files may include personal information obtained from a client.
- Working paper files and other files containing, for example, copies of personal tax returns are retained by the firm for a minimum of ten years, or longer subject to our file retention policies.

- The personal information collected from a client during the course of a professional service engagement may be:
 - shared with the firm's personnel participating in such engagement;
 - disclosed to partners and employees within the firm to the extent required to assess compliance with applicable professional standards and rules of professional conduct and the firm's policies, including those providing quality control reviews of work performed;
 - provided to members of the organization's audit committee and board of directors, and others in the company that might not otherwise have access to the information, in the course of communicating aspects of the results of our audit; and
 - provided to external professional practice inspectors (e.g., representatives of the provincial institute of chartered accountants) who, by law, professional regulation or contract have the right of access to the firm's files for inspection purposes

Principle #6: The firm endeavours to keep accurate, complete and up-to-date, personal information in its possession or control, to the extent required to meet the purposes for which it was collected.

- Individual clients are encouraged to contact the firm's engagement partner in charge of providing service to them to update their personal information.

Principle #7: The firm protects the privacy of personal information in its possession or control by using security safeguards appropriate to the sensitivity of the information.

- Physical security (e.g., restricted access) is maintained over personal information stored in hard copy form. Partners and employees are authorized to access personal information based on client assignment and quality control responsibilities.
- Authentication is used to prevent unauthorized access to personal information stored electronically.
- No files or other materials containing personal information are entrusted to third party service providers (e.g., a provider of paper based or electronic file storage).

Principle #8: The firm is open about the procedures it uses to manage personal information.

- Up-to-date information on the firm's privacy policy can be obtained from the firm's Privacy Officer (see contact information under principle 1).

Principle #9: The firm responds on a timely basis to requests from clients about their personal information which the firm possesses or controls.

- Individual clients of the firm have the right to contact the engagement partner in charge of providing service to them and obtain access to their personal information. Similarly, authorized officers or employees of organizations that are clients of the firm have the right to contact the engagement partner in charge of providing service to them and obtain access to personal information provided by that client. In certain situations, however, the firm may not be able to give clients access to all their personal information. The firm will explain the reasons why access must be denied and any recourse the client may have, except where prohibited by law.

Principle #10: Clients may challenge the firm's compliance with its Privacy Policy.

- The firm has policies and procedures to receive, investigate and respond to clients' complaints and questions relating to privacy.
- To challenge the firm's compliance with its Privacy Policy, clients are asked to provide an email message or letter to the firm's Privacy Officer (see contact information under principal 1 above). The firm's Privacy Officer will ensure that a complete investigation of a client complaint is undertaken and will report the results of this investigation to the client, in most cases, within 30 days.