Hawkins & Co.
ADVISORS | CPAs

PRIVACY POLICY RELATING TO PERSONAL INFORMATION

Introduction

Hawkins & Co. Accounting Professional Corporation ("we" or "the firm") collects, uses and discloses personal information in the possession, or under the control, of its clients and employees to the extent required to fulfill its professional responsibilities and operate its business. We are committed to maintaining the privacy of personal information provided by our clients and employees and protecting all personal information in our possession or control. This Privacy Policy sets out the ten principles and procedures that we follow in meeting our privacy commitments to our clients and employees, and complying with the requirements of federal and provincial privacy legislation.

Principle #1 – ACCOUNTABILITY

We are accountable for all personal information in our possession or control. This includes any personal information that we receive directly (from clients who are individuals, and from employees) or indirectly (through clients that are organizations, such as corporations, government entities or not-for-profit organizations).

From time to time, we may be engaged to act as consultants or subcontractors to other professional service firms. To the extent that they apply, all statements in this policy document apply equally to personal information of clients or employees of such firms as to our own clients or employees.

We have:

- established and put into effect policies and procedures aimed at properly protecting personal information;
- educated our partners and employees regarding our privacy policy and their role and responsibilities in keeping personal information private; and
- appointed our Privacy Officer [Julian Hawkins, FCPA, FCA] to oversee privacy issues at the firm.

If you have any questions about this firm's privacy policies and practices, the firm's Privacy Officer can be reached by email at jules@hawkins-accounting.ca, by phone at 519 997 2900, by fax at 519 997 2901, or by mail at Hawkins & Co. Accounting Professional Corp., 2090 Wyandotte St E Suite 201, Windsor ON N8Y 5B2.

Hawkins & Co.
ADVISORS | CPAs

Principle #2 – IDENTIFYING PURPOSES

We identify the purposes for which we collect personal information from clients or employees before we collect it.

Where we collect personal information from clients, we use and disclose 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 – CONSENT

We obtain a client's consent before collecting personal information from that client.

The terms and conditions of a professional services engagement are documented in the engagement letter for that engagement. These terms and conditions include an explanation about how we may use and disclose your personal information. By signing the engagement letter, you will be providing your consent to the collection, use and disclosure described in the terms and conditions.

Engaging our firm to prepare personal tax returns constitutes implicit consent to collect and use such information. It also constitutes implicit consent for us to disclose such information to tax authorities, if required to respond to an inquiry, review or audit relating to a client's tax return.

Such personal information may include – but is not limited to – the following:

- home addresses and telephone numbers
- personal identification numbers (e.g., social insurance numbers, credit card numbers)
- financial information (credit ratings, payroll information, personal indebtedness)
- personal information (e.g., date of birth, employment history, references to criminal records)
- information relating to medical conditions, procedures or treatments
- information related to race, religion, sexual preference or identification, or receipt of government benefits

Employment candidates will also be advised of the purposes for which their personal information is being collected and will be provided an opportunity to consent to the collection, use and disclosure as described.

You always have the option not to provide your consent to the collection, use and distribution of your personal information, or to withdraw your consent at a later stage. Where a client chooses not to provide us with permission to collect, use or disclose personal information, we may not have sufficient information to provide him or her (or a related organization) with our services. Where a candidate for employment chooses not to provide us with permission to collect, use or disclose personal information, we may not be able to employ him or her.

Principle #4 – LIMITING COLLECTION

The partners and staff involved in an engagement 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 report on a client's financial information, or to facilitate the completion of special projects as engaged by the client. Such personal information may be a significant component of various transactions and events affecting the financial information under engagement, and may be subjected to confirmation, testing, analyses and such other procedures as may be necessary to complete the engagement in accordance with relevant professional standards.

We also collect and may use personal information to enable us to provide you through various channels with information that we believe are of interest to you. This includes such matters as:

- new services we provide,
- conferences and other professional development courses we hold,
- notice of changes in the law or accounting practices that may be relevant or of interest to you, and
- other professional or business developments.

If you do not wish to receive such information, you may opt out by sending an email to info@hawkins-accounting.ca, and we will discontinue sending you information other than in regard to your account.

We collect only that personal information required to provide our professional services and to operate our business, as described above. We collect it by fair and lawful means.

Principle #5 – LIMITING USE, DISCLOSURE & RETENTION

We use or disclose personal information only for purposes for which we have consent, or as required by law.

We may also disclose personal information without consent:

- to comply with a subpoena, a warrant or an order made by a court or other body with appropriate jurisdiction or to comply with rules of conduct required by regulatory bodies. It is important to note that accounting firms are not protected by client/solicitor privileges.

- to a government institution that has requested the information, identified its lawful authority, and indicates that disclosure is for the purpose of enforcing, carrying out an investigation, or gathering intelligence relating to any federal, provincial or foreign law; or suspects that the information relates to national security or the conduct of international affairs; or is for the purpose of administering any federal or provincial law.

- to an investigative body or government institution on our initiative when we believe the information concerns a breach of an agreement, or a contravention of a federal, provincial, or foreign law, or we suspect the information relates to national security or the conduct of international affairs. In certain situations, we may be under a legal obligation to do this.

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 papers are safeguarded against inappropriate access, as discussed under Principle 7.

The firm retains personal information only as long as necessary to fulfill its purposes. Working paper files and other files containing, for example, copies of personal tax returns are retained for the time period required by law and regulation or for the time period as specified in our policy governing retention of client information.

We regularly and systematically destroy, erase, or make anonymous personal information no longer required to fulfill the identified collection purposes, and no longer required by laws and regulations.

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 team members 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 providing quality control reviews of work performed;

- provided to external professional practice inspectors, who by professional regulation have the right of access to the firm's files for inspection purposes. Such inspectors are required to comply with privacy requirements comparable to those contained in this policy.

Principle #6 – ACCURACY

We endeavour to keep accurate, complete, and up-to-date, personal information in our possession or control, to the extent required to meet the purposes for which it was collected.

Individual clients are encouraged to contact a partner of the firm, if they need to update their personal information.

Principle #7 – SAFEGUARDS

We protect the privacy of personal information in our possession or control by using security safeguards appropriate to the sensitivity of the information. We conduct periodic audits to evaluate the effectiveness and application of these safeguards.

Safeguards in place include, but are not limited to, the following:

- Partners and employees are authorized to access personal information based on client assignment and quality control responsibilities. An employee's access to any such information is revoked immediately upon departure from employment. This includes access to information that may be potentially held on or accessed through an employee's personal device (eg. emails sent via smartphone).

- Information stored in hard copy form is protected by physical security measures (e.g., restricted access to our office).

- Personal information stored electronically on our network or "in the cloud" is protected by authentication procedures, to validate the identity of the person seeking access. Whenever possible, these access procedures include two-factor authentication and use of biometric controls.

- Any personal information received or sent over the Internet (including by email) is transmitted via secure portals or websites whenever possible, and/or is encrypted or password-protected before transmission.

Violations of this policy by employees may be considered cause for disciplinary action, potentially including termination of employment.

Where we entrust files and other materials containing personal information to a third party service provider (e.g., an external consultant or subcontractor), we obtain appropriate assurance that the level of protection of personal information provided by the third party is equivalent to that of the firm. Such third parties are typically also professional service firms, and are subject to the same regulatory and legislative obligations as we are.

Hawkins & Co.
ADVISORS | CPAs

Principle #8 – OPENNESS

We are open about the procedures we use 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 – INDIVIDUAL ACCESS

We respond on a timely basis to requests from clients and employees about their personal information which we possess or control.

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 – CHALLENGING COMPLIANCE

Clients or employees 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 send an email message or letter to the firm's Privacy Officer (see contact information under Principle 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.

Clients have the right to refer the matter to our professional body, CPA Ontario, if the matter is not resolved to their satisfaction.

Update version: Oct 2019