Generally Accepted Privacy Principles are founded on the following privacy objective:

Personal information is collected, used, retained, and disclosed, and disposed of in conformity with the commitments in the entity's privacy notice and with criteria set forth in Generally Accepted Privacy Principles issued by the AICPA/CICA.

The following are the 10 Generally Accepted Privacy Principles:

1. Management
2. Notice
3. Choice and Consent
4. Collection
5. Use, Retention and Disposal
6. Access
7. Disclosure to Third Parties
8. Security for Privacy
9. Quality
10. Monitoring and Enforcement

The Firm's Privacy Policy, which follows, is based on the above 10 Generally Accepted Privacy Principles:

Introduction

Leckie & Associates LLP 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 to operate its business. The Firm is committed to maintaining the privacy of personal information provided by its clients and to protecting all personal information in its possession or control. This Privacy Statement sets out the principles and procedures that the Firm follows in meeting its privacy commitments to its clients and in complying with the requirements of federal and provincial privacy legislation.

Principle #1 - Accountability:

The Firm is accountable for all personal information in its possession or control. This includes any personal information the Firm receives 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 principals and employees regarding its privacy policies, and of their roles and responsibilities in keeping personal information private; and
- Appointed a Privacy Officer to oversee privacy issues within the Firm.

If you have any questions about the privacy policies and practices of the Firm, Greg M. Dewing, CPA CA CGA, the Privacy Officer of the Firm, can be reached by email at **greg.dewing@leckiecpa.com**, by telephone at 780-875-9293 and by letter at PO Box 11706 Lloydminster, AB T9V 3C1.

Principle #2 – Identifying Purposes:
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 personal information only to provide the requested professional services to those clients. The types of information that may be collected for this engagement, and the purpose for which it is collected, are set out under Principles 3 and 4 of the privacy statements.

Personal information attached to clients' email accounts will be retained on our secure servers for archiving and future requirements.

Personal information uploaded by clients to the Firm's portal site will be retained on our secure servers for archiving and future requirements.

We collect your IP addresses on our portal site for system administration, including diagnosis of problems with the firm's servers and administration of the firm's portal site.

Our portal site uses cookies. A "cookie" is information that our website places on your hard drive so that it can remember information about you the next time you visit our website (so that we can provide you with personalized services), measure traffic patterns (so that we can learn which browsers are commonly used), and estimate audience size (so that we can know which, visitors have seen particular parts of the website). You can still navigate through our website without the use of cookies, but your access and the functionality of the website may be limited.

Principle #3 – Consent:
The Firm obtains client consent before collecting personal information from that client.

The Terms and Conditions of every professional services engagement are documented in each Engagement Letter. These Terms and Conditions include an explanation about how Leckie & Associates LLP 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.

Such personal information could include:

- Home addresses
- Home telephone numbers
- Personal identification numbers
- Financial information
- Personal information
- Information linked to the type of client

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 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 enough information to provide you 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 you.

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

The partners and staff involved in an engagement will access only the information required to complete that engagement in accordance with generally accepted accounting standards or a special project or to deal with Firm matters such as invoicing and general correspondence.

Principle #5 – Limiting Use, Disclosure & Retention:
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 for the time required by law and regulation. Working papers are safeguarded against inappropriate access, as discussed under Principle 7.

The personal information collected from a client during a professional service engagement may be:

- Shared with Firm personnel participating in such engagement;
- Disclosed to partners and employees within the Firm to the extent required to assess compliance with applicable professional standards, rules of professional conduct, and the Firm's policies, and to conduct quality control reviews of the work performed;
- In the case of an audit engagement, provided to the members of an audit committee and to the board of directors of an organization, and others in the company that might not otherwise have access to the information, during communicating certain aspects of the results of our audit; and
- Provided to external professional practice inspectors (e.g., representatives of the Canadian Public Accountability Board, or the Institute of Chartered Professional Accountants of Alberta), who by law, professional regulation, or contract, have the right of access to Firm files for inspection purposes.

The personal information collected from a client during a professional service engagement may be disclosed without consent only for the following reasons:

- 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 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 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.

We also use it 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,
- Notices of changes in the law or accounting practices that may be 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 **main@leckiecpa.com** or by advising the Firm's engagement partner in charge of providing service to you and we will discontinue sending you information other than in regard to your account.

The Firm regularly and systematically destroys, erases, or makes anonymous personal information that is no longer required to fulfill the above collection purposes, and is no longer required by laws and regulations.

Principle #6 – Accuracy:
The Firm endeavors 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 engagement partner of the Firm in charge of providing services to them to update their personal information whenever changes are required.

Clients who have signed consent to set-up and use a portal account on the Firm's portal site are responsible for notifying the Firm's engagement partner in charge of providing service to them of any changes to their user access profile immediately so that the information can be updated appropriately.

Principle #7 - Safeguards
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, locked rooms and filing cabinets) 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 on our secure servers, which are maintained and located in a restricted access location.

For files and other materials containing personal information entrusted to a third-party service provider (e.g., a provider of paper based or electronic file storage), the Firm obtains appropriate assurance to affirm that the level of protection of personal information by the third party is equivalent to that of the Firm.

Principle #8 - Openness
The Firm is open about the procedures it uses to manage personal information.

Up-to-date information regarding the privacy policy of the Firm can be obtained from the Privacy Officer of the Firm (see contact information under Principle #1 of this Privacy Statement).

Principle #9 – Individual Access
The Firm responds on a timely basis to requests from clients about their personal information that the Firm possesses or controls.

Individual clients of the Firm have the right to contact the engagement partner in charge of providing services to them to 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 services to them to 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. In such situations, 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 may challenge the compliance of the Firm with its Privacy Policy.

The Firm has policies and procedures to receive, investigate, and respond to client complaints and questions relating to privacy.

To challenge the compliance of the Firm with its Privacy Policy, clients are asked to provide an email message or letter to the Privacy Officer of the Firm (see contact information under Principle #1 of this Privacy Statement). The Privacy Officer will ensure that a complete investigation of the client complaint is undertaken and will report the results of this investigation to the client, in most cases, within 30 days.
A copy of the firm's privacy policy is kept on the firm's website at **www.leckiecpa.com** and can be accessed by our clients, staff and the public at any time.

The firm's policies and procedures to receive investigate and respond to client complaints and questions relating to privacy are detailed in the "Privacy Policy Procedures" section later in this manual.