In effect and as amended to November 1, 2018

McATEER GROUP OF COMPANIES

PRIVACY POLICY: POLICIES AND PRACTICES ("Privacy Policy")

Overview

The McAteer Group of Companies (McAteer) is engaged in the provision of third party administration services for sponsors of health, pension, vacation pay, legal services, scholarship, training and other workplace benefit plans. We also provide consulting and other services to benefit plans sponsors (clients). Our clients reside in every Province and Territory of Canada. McAteer is also an employer of over 70 employees in two Provinces – Alberta and Ontario.

Privacy legislation directly impacts the clients of McAteer (they all should have privacy policies of their own) and our own business operations.

Other Policies related to Privacy

This Privacy Policy must be read in conjunction with Schedule 1 to this Policy.

Privacy

Privacy is a concept that encompasses confidentiality but extends beyond it. Privacy addresses the way in which we collect, use and disclose personal information, the right of an individual to control the use, collection and disclosure of his or her personal information, the right to have access to his or her personal information and the right to have it corrected, if necessary.

Legislation

If there is no provincial privacy legislation governing the activities of a Province, the default legislation is the Federal *Personal Information Protection and Electronic Document Act* (PIPEDA). The Federal Privacy Commissioner has recognized the legislation of Quebec, Alberta and British Columbia as "substantially the same" which means that the legislation in those provinces is applicable to McAteer's and clients' operations within those Provinces. In all other provinces, PIPEDA prevails. Importantly, Ontario's Bill 31 – *The Personal Health Information Protection Act, 2004* – governs the protection of health information.

Since 2000, McAteer has been guided by, and informed and educated its employees about, the requirements of the Canadian Standards Association (CSA) Model Code for the Protection of Personal Information.

Each employee of McAteer has received a personal copy of the CSA model code (The 10 Principles). Since January 1, 2001, each new employee of McAteer receives the McAteer Group of Companies Privacy Policy: Policies and Practices together with their employment letter. It forms a part of the function description for each position. The 10 Principles and the McAteer Privacy Policies and Practices are also posted in several locations throughout our offices to serve as an ongoing reminder that privacy and protection of Personal Information is integral and essential to our work. The 10 Principles are attached.

McAteer has a policy for the reporting of privacy breaches to the applicable authorities.

Essential Privacy Policy Concepts

The hallmarks of the McAteer Privacy Policy include:

- All employees are aware of what defines Personal Information.
- All employees have respect for the Personal Information in our possession, whether that information is received in a written, electronic or verbal form.
- All new employees are provided with the most current McAteer Group of Companies' Privacy Policy: Policies and Practices with their employment letters and are required to sign a copy of the Policy document acknowledging receipt and understanding of the document before the first date of employment with us.
- All employees are required to "sign off" in writing on compliance with our Privacy Policy at least once per year.
- Breaches of the McAteer Privacy Policy may result in termination of employment.
- Access to filing areas is secure.
- Only authorized users with secure passwords have access to the information on the computer system.
- Managers are responsible for the monitoring of the care of Personal Information (without restriction as to their department – ie they are responsible for observing how Personal Information is being protected everywhere) including the access of Personal Information hard copy and computer records and taking action whenever necessary.
- Employees who do not have direct responsibility for the collection, use, disclosure or storage of Personal Information are not permitted to accept such Personal Information from any party. For example, clerical employees (i.e. receptionists) are not permitted to view Personal Information such as disability details or change of marital status, etc. Information received verbally must be directed to the administration employees responsible for the safekeeping of Personal Information.
- To the greatest extent possible, employees expecting highly sensitive Personal Information (such as health records) will advise the sender to provide the correspondence "Private" and this information, when received will be given directly to the responsible employee without opening the correspondence.

- Any correspondence sent electronically containing personal information will be sent in encrypted manner.

- Discussions with clients, including those with plan members, that include or may include, Personal Information will be conducted in private. Discussions with plan members or others about claims, benefit entitlement, etc. will not be conducted in main office areas.

- Member authorizations to release Personal Information to a third party (other than a supplier to the plan such as an insurer or custodian, etc.) will not be accepted, except under Court Order unless reviewed and approved by a Manager.

- Discussions with and between employees about plan members' Personal Information will be limited to those employees who must be part of the discussion and such discussions will take place in a formal and private environment.

- Employees will not ask members for their Social Insurance Number (SIN) as an identifier on phone calls or in consultations (use last name, first name, plan member ID, postal code, or other unique identifiers)

- Employees will not leave personal information (including details about the member's status such as a relationship breakdown, adding or deleting a dependant/spouse, change in beneficiary etc.) on a client or plan member's voicemail. A message will be left asking the person to call our office.

- Employees will ensure that any Personal Information in their possession is locked in their desks such that it is not accessible during times when the office is closed.

- Managers will monitor transactions including records belonging to their departments to ensure that they are being handled in compliance with this Policy (for example, records being sent to off-site storage are to be taken off property expeditiously and may not be left unprotected unless the collection of these records is imminent).

- Managers may also inspect employee work areas, audit telephone calls, emails and conversations and take other reasonable steps at any time for the purpose of verifying compliance with our Privacy Policy and standards.

- Company computers and laptops are not to be used for personal use. All information contained on company computers, including company emails, is considered company property, and will be accessed at any time. Examples of this include, but is not limited to; accessing email accounts during employee absences, forwarding email accounts to other employees for response to members, and accessing files and letters on employee computers.

- Plan members and other, non-staff, will not have access to administration areas unless they are under the direct control of a responsible employee.

- Employees who meet with plan members or other parties will ensure that any Personal Information not relevant to the meeting is put away during the discussion.

- Third parties retained, or under consideration, by McAteer must provide their written privacy policy statement before they are permitted to handle any Personal Information (this includes mailing houses, custodians, banks, insurers, financial institutions, etc.). McAteer will engage only those third parties with a privacy policy substantially similar our Policy.

- Record retention policies will be reviewed in conjunction with clients and third parties to ensure that only the Personal Information that is necessary is retained and that unnecessary Personal Information is either not collected or, if collected, is destroyed securely when it is no longer needed.

- Paper documents to be destroyed are to be placed in the shredding locations available throughout the office at the end of each working day. Employees are not to place business documents of any kind in regular garbage disposals. Paper shredding providers are to provide a certificate of shredding to McAteer at the end of each site attendance.

- Secure electronic record storage will be used to the greatest extent possible to ensure greater privacy protection and document control.

- Only password protected mobile devices (e.g. laptops, mobile phones) can be used for company communications. These passwords must be updated regularly.

- Recommendations for better security are always welcome and should be given to Kimberly Houston or Debbie Pawlick.

- Breaches of the privacy policy must be reported by any staff who knows of the breach. The policy for reporting breaches is to be followed.

PERSONAL INFORMATION COLLECTION, USE, DISCLOSURE, CORRECTION AND ACCOUNTABILITY

1. **McAteer as an Employer**

   With respect to the Personal Information in our possession due to our role as an employer, written employee consent will be required in connection with the collection, use, retention and disclosure of Personal Information. We review, and will continue to review, our operations to ensure that:

   - Only necessary Personal Information is collected, used and disclosed and retained.

   - Employees are notified, whenever possible, if their Personal Information is to be disclosed (for example, employees must give written consent for electronic payroll services since the payroll service will have access to Personal Information). Personal Information may need to be disclosed in an emergency or by law.

   - We assure that our third-party suppliers have appropriate privacy policies before we agree to disclose Personal Information about our employees.

   - Personal Information records are maintained in a safe and secure environment, with restricted access. Obsolete records are destroyed in a secure manner.

   - Personal Information records are accurate and complete and employees have every opportunity to review their Personal Information on file with us and to make any corrections.

   - Our employees have access to a Privacy Officer to review any concerns or complaints related to the privacy of Personal Information.

   - Our Privacy Officers are responsive to employee inquiries about privacy issues and will

cooperate with inquiries and be transparent about practices.

Employee Privacy at Work

We respect your privacy and will not disclose Personal information about you without your permission, unless compelled to do so by law.

We reserve the right to conduct, at any time, a search of any employee's work area and property and materials on our premises. We reserve the right to inspect employees' desks, file cabinets, computer, e-mail, memory sticks, hard drive, or any package carried by employees in or out of our facilities. We expressly reserve the right to monitor telephone, social media, facsimile, e-mail, and/or other electronic communications. Consent to such inspections is a condition of employment, or continued employment, with us. Any employee who fails or refuses to undergo an inspection will be subject to disciplinary action, up to and including immediate termination of employment.

Employee Privacy Education and Information

All employees have had, and will continue to be given, education and information about privacy legislation, including updates to the McAteer Group of Companies Privacy Policy: Policies and Practices. All Supervisors and Managers are responsible for ensuring that the appropriate privacy standards are observed.

2. **McAteer as a Service Provider**

Due to the nature of our business, we possess the Personal Information of others. We encourage our clients to review the processes we have for the effective administration of their Personal Information. It is expected that clients will have their own privacy policies. As noted above, since our employees have worked under the 10 Principles since 2001, it is expected that any privacy policy implemented by a client will not introduce elements that are unfamiliar to our employees.

Upon request by the client, we review all documents and procedures in place for the applicable client. Upon request, we make suggestions for changes.

Client Privacy Policies

In general, it is expected that our clients will develop privacy policies that include the following standards. The standards are included in our Policy to provide greater insight, education and direction about the management of Personal Information:

a) Plan members, or those covered by the plan (health, pension etc.), will have to provide their written consent to the collection, use, disclosure and retention of their Personal Information. Member authorizations to release Personal Information to a third party (other than a supplier to the plan such as an insurer or custodian, etc.) will not be accepted, except under Court Order. Consent wording should be clear to ensure the plan member understands what is being asked of him/her.

b) Clients will collect only the Personal Information necessary for the effective administration of the plan (for example if wage information is not necessary for the administration of a plan then it should not be collected).

c) Other parties engaged by clients to provide services (such as a custodian, insurer or bank) will have written privacy policies in place that will continue to protect the Personal Information collected by the plan.

d) Clients will not retain Personal Information after the time when it is no longer needed or relevant for the effective administration of the plan.

e) Plan members will have reasonable access to their Personal Information retained by the plan. If any of the Personal Information kept by the plan is inaccurate or incomplete, the plan will review the information and make necessary corrections to the Personal Information.

f) Plan documents such as forms, applications, statements, cheques, etc. will have the proper privacy practices disclosure.

In the development of their privacy policies practices, clients may look to us to provide:

a) Systems that ensure that the Personal Information that is collected is accurate and current.

b) Assurance that Personal Information collected is protected against unauthorized use, disclosure, copying, modification or destruction.

c) Assurance that redundant or obsolete Personal Information is effectively discarded when it is no longer useful. The destruction of client records is not at our discretion. Clients should have record retention policies. Our employees must keep client records in good order.

Clients may also wish to engage a senior McAteer employee (often the Executive Administrator or Recording Secretary) to act as their Privacy Officer. The person designated as the client's privacy officer is responsible for ensuring that the client's privacy policy is communicated to the appropriate McAteer employees and others as applicable.

If the client does not engage a McAteer employee as their designate for privacy related matters, our employees will still refer to the on-site McAteer employee who acts as the applicable Executive Administrator or Recording Secretary in connection with matters to do with privacy. In the event that the client's Executive Administrator or Recording Secretary is not available to respond to a privacy-related matter, then employees will refer the matter to our Privacy Officer. Our Privacy Officer may consult with other employees.

DEFINITIONS

"Record"

Record means any record of information however recorded, whether in printed form, on film, by electronic means, or otherwise, and includes:

- correspondence, a memorandum, a book, a plan, a map, a drawing, a diagram, a pictorial or graphic work, a photograph, a film, a microfilm, a sound recording, a videotape, a machine-readable record, any other documentary material, regardless of physical form or characteristics, and any copy thereof;

- any record that is capable of being produced from a machine-readable record under the control of McAteer by means of computer hardware and software or any other information

storage equipment and technical expertise normally used by the Company, or to which the Company can reasonably gain access;

- e-mail records, including additional/forwarded copies.

“Personal Information”

Personal information is defined in PIPEDA as recorded information about an identifiable individual and includes but is not limited to the following information:

- name, race, national or ethnic origin, colour, religion, age, sex, sexual orientation, or marital, family or social status of the individual;
- information relating to employment including disciplinary actions, education or salary history;
- information relating to the medical records, health information, psychiatric, psychological history, prognosis, condition, treatment or evaluation;
- any identifying number, for example, Social Insurance Number (S.I.N.), symbol or other particular assigned to the individual;
- date of birth;
- home address and/or telephone number;
- the individual’s name where it appears with or reveals other personal information;
- correspondence sent to McAteer by the individual that is implicitly or explicitly of a private or confidential nature and replies to that correspondence that would reveal the contents of the original correspondence;
- Personnel or criminal record, credit and loan records.

However, information about individuals acting in their business or professional capacity such as name and title, work address (including office location), work telephone number, work e-mail address, etc. is NOT personal information.

The *Ontario Personal Health Information Protection Act*, 2004 defines personal health information as:

> *“Certain information about an individual, whether living or deceased and whether in oral or recorded form. It is information that can identify an individual and that relates to matters such as the individual’s physical or mental health, providing of health care to the individual, payments or eligibility for health care in respect of the individual, the donation by the individual of a body part or bodily substance and the individual’s health number.”*

Privacy Officers

Kimberly Houston is the Privacy Officer for Ontario operations. Debbie Pawlick, CEBS is the Privacy Officer for Alberta operations. Their contact information is below. The responsibilities of the Privacy Officers include:

- Acting as role models in the protection of personal information.
- Understanding the applicable privacy legislation.
- Communicating with Privacy Officers about emerging practical issues regarding privacy protection (this ensures that our Privacy Policy is a living document and is amended as new information is available and situations are encountered).
- Communicating with employees about changes to the applicable l legislation.
- Assessing the impact of privacy legislation for McAteer as an employer and as a provider of services.
- Drafting, discussing and implementing privacy policies and procedures.
- Recommending amendments to the McAteer Group of Companies' Privacy Policies and Practices.
- Accountability for privacy readiness, employee education, modifications to privacy related policies and procedures and addressing complaints.
- Responding to employees, members, trustees, union representative or other inquiries about the McAteer Group of Companies' Privacy Policy: Policies and Practices.
- Carrying out any disclosure requirements under the applicable privacy legislation including privacy breaches.

Kimberly can be reached at khouston@mcateer.ca or at 905-946-8655 ext 257. Debbie can be reached at dpawlick@mcateer.ca or at 780-452-1331 ext. 270.

COMPLAINTS

If any privacy related complaints are received in connection with a benefit plan, and assuming the client has engaged McAteer as the designated Privacy Officer, the complaint should be referred first to the Executive Administrator or Recording Secretary of the plan. These persons will be responsible for investigating and responding to the complaint within the time permitted by legislation.

PRIVACY BREACHES

A "privacy breach":

- is unauthorized collection, use or disclosure of someone's personal information, in contravention of the PIPEDA or the *Ontario Personal Health Information Protection Act;*

- may affect an individual or a group;

- may be reported by an Employee, or by someone external to McAteer, including A federal or provincial privacy commissioner who may have received a complaint.

If a privacy breach related to McAteer's role as an employer is suspected or confirmed, immediately report it to the Privacy Officer. See Schedule 1 for further details.

REVIEW OF PRIVACY POLICIES AND PRACTICES

Training and Education

We believe in equipping responsible persons with the appropriate tools for the management of personal information. Ongoing training about the responsibility for the safety of personal information is provided to all staff persons. As recommended by PIPEDA, training and education will include, but are not limited to, the following subjects;

- Security Safeguards
- Policies and Procedures for;
- Assessment and Response
- Record-Keeping
- Reporting, Notifications, and Disclosures
- Legal Privilege
- Contracts with Data Processors

Audit of Controls

Managers and Privacy Officers have the responsibility for audit of the privacy controls. These audits may, and should be conducted randomly and non-compliance reported to the Privacy Officers. Audits of controls will also be conducted formally by the Privacy Officers no less than once per year. Corrections to operations will be made as necessary.

Annual Sign-Off by McAteer Staff

McAteer staff will be required, on an annual basis, to sign-off, with respect to each person's compliance with this Policy.

Transparency

This Policy will be made available to all employees on the McAteer Group of Companies All Staff Drive and in the Staff Handbook.

Review

This Policy will be reviewed bi-annually or more frequently if necessary.

Amendments to the McAteer Group of Companies' Privacy Policy: Policies and Practices will be communicated. The updated McAteer Group of Companies' Privacy Policy: Policies and Practices will be posted in suitable common areas in all McAteer offices. Employees will be given a personal copy of our Privacy Policy.

The McAteer Group of Companies

10 PRINCIPLES

The new privacy law is based upon the 10 principles of the Canadian Standards Association's Model Code for the Protection of Personal Information, a code that was agreed upon by governments, businesses, and consumers in 1995.

The 10 Principles of the CSA Model Code are:

Accountability - An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles. For the McAteer Group of Companies those persons are Susan Bird, President, Richard McAteer, Vice President, Kimberly Houston, Managing Director, and Debbie Pawlick, Supervisor-Edmonton Office.

Identifying Purposes – The purpose for which personal information is collected shall be identified by the organization at or before the time the information is collected.

Consent – The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Limiting Collection – The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

Limiting Use, Disclosure, and Retention – Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

Accuracy – Personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.

Safeguards – Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

Openness – An organization shall make readily available specific information about its policies and practices relating to the management of personal information.

Individual Access – Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Challenge Compliance – An individual shall be able to address a challenge concerning compliance with the above principles to the designed individual or individuals accountable for the organization's compliance.

McAteer Group of Companies

PRIVACY POLICY SCHEDULE 1
Mandatory Notification Requirements of PIPEDA
Effective November 1, 2018

Organizations subject to the federal *Personal Information Protection and Electronic Documents Act* ("PIPEDA") must notify affected individuals of a breach to the confidentiality of their personal information that results in real **risk of significant harm** to them.

PIPEDA regulations define **significant harm** as including "bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property."

The regulations require organizations to report all applicable breaches to the Privacy Commissioner of Canada ("the Commissioner") and to maintain records of all breaches involving personal information including those that do not meet the **real risk of significant harm** threshold.

Background

The factors that are relevant in determining whether there is a **real risk of significant harm** to an individual include

a. the sensitivity of the personal information involved,
b. the probability that the personal information has been, is being or will be misused,
c. and any other prescribed factor. There are currently no other prescribed factors.

PIPEDA defines a "**breach of security safeguards**" as the loss or disclosure of personal information or the unauthorized access to personal information resulting from a breach of the organization's security safeguards or from its failure to establish such safeguards.

Impact on the Plan/Plans

In the event of an applicable breach, the Plan must:

- report the breach to the Commissioner (see Plan Notice to Commissioner below);
- notify the affected individuals; and
- notify government institutions, or other organizations if the Plan believes that the other organizations may be able to reduce the risk of harm to the affected individuals.

Penalties

If the Plan fails to report privacy breaches to the Commissioner, fails to notify affected individuals of breaches affecting their personal information or fails to maintain records of such breaches it could be subject to fines of up to $100,000.

Analysis of a Breach Incident

The applicable McAteer Group of Companies' Privacy Officer will be responsible for analyzing a possible or actual breach. The components of the analysis will be documented and will include:

- The date of the incident?
- When and how the incident was discovered?
- Where did the incident take place?
- What caused the incident?
- Is the breach contained?
- Other than the Privacy Officer, is any other staff person assisting?
- Is the breach a criminal matter? Do police need to be involved?
- Does an insurer need to be notified?
- Do others (other than the privacy commissioner as set out below) need to be informed? I.e. financial institution, credit agency?
- Are the documents related to the breach protected (ie not destroyed)?
- What personal information was breached?
- The number of individuals affected?
- What loss to the affected individual could happen? [identity theft, financial loss, employment, physical harm, embarrassment, reputation]
- If personal information was lost, is it recovered?

- Was this an electronic breach or a “paper” breach?
- Could the same breach happen again? If so, how do we protect against another similar breach?
- What harm could come to The McAteer Group of Companies as a result of the breach?
- What are our legal obligations including those in a client agreement governing breaches?
- If notification of the affected individual is necessary, how will this be done [by phone, by mail, in person]? If this is a larger breach impacting more than one person should notification be by social media [ie website]?
- Should an expert in the matter be retained?

Notice to Commissioner

PIPEDA requires that a report to the Commissioner be made as soon as feasible after the Plan determines that a privacy breach that resulted in a **real risk of significant harm** has occurred. The regulations require the report must be in writing, and be submitted via a secure means of communication, such as an encrypted email.

The Plan communication must contain at least the following:

- a description of the breach and its cause, if known;
- the date, or the period or approximate period, of the breach;
- a description of the personal information involved to the extent that it is known;
- the number, or approximate number, of individuals affected by the breach;
- a description of the steps taken by the Plan to reduce the risk of harm to those individuals;
- a description of the steps taken by the Plan, or intended to be taken, to notify the affected individuals; and,
- the contact information of the Plan’s Privacy Officer who can answer the Commissioner's questions about the breach.

The regulations recognize that the full extent of a breach may not be known immediately. They permit, but do not require, the Plan to provide new information to the Commissioner following the initial reporting of a breach.

Notice to Individuals

PIPEDA requires that notice of a breach must normally be provided to affected individuals directly and as soon as feasible after the Plan determines that a breach has occurred. Notices must contain sufficient information to allow an individual to understand the significance to them of the breach and to take steps, where possible, to reduce the risk of harm or mitigate such harm.

The regulations require that at least the following information be included in such notices:

- a description of the breach;
- the date, or the period or approximate period, of the breach;
- a description of the personal information which was compromised to the extent that it is known;
- a description of the steps taken by the Plan to reduce the risk of harm to affected individuals;
- a description of the steps that affected individuals could take to reduce the risk of harm to them or mitigate such harm; and,
- the contact information of the Privacy Officer who will answer questions about the breach.

The regulations provide that notice may be given in person, by telephone, mail, email or any other form of communication that a reasonable person would consider appropriate in the circumstances. The form of notice should be documented so the Plan can address any future claim that no notice, or insufficient notice, was provided.

The regulations also provide that affected individuals can be notified indirectly if direct notice would likely cause further harm to the individual, cause undue hardship for the Plan/Plans, or if the Plan does not have contact information for the affected individual. Indirect notice must be given by public communication or by a similar measure that could reasonably be expected to reach the affected individuals such as a newspaper advertisement, posting in the workplace or on a relevant website.

The method of notice will be determined by the Privacy Officer and the Plan via the Recording Secretary with the Steering Committee.

Breach Record Keeping

PIPEDA requires that the Plan maintain records of all breaches of its security safeguards, including those that do not meet the **real risk of significant harm** threshold, for 24 months from the date the Plan/Plans determined that a breach had occurred. These records must be available to the Commissioner upon request and must contain sufficient information for the Commissioner to determine whether the Plan complied with its notification and reporting obligations.

The records of breaches which did not satisfy the **real risk of significant harm** threshold should indicate how that determination was made.

Breach records are destroyed after 24 months unless the matter is the subject of known litigation.

Depending on the information breach the Plan may pay the cost of cost of credit monitoring for affected individuals if the confidentiality of their financial information is breached. Different steps may be required if the confidentiality of personal medical information is breached. The determination will be made on a case by case basis by the Steering Committee of the Board of Trustees.

Encrypted Data

It is the policy of the Plan administrator to send confidential data in an encrypted format. However many members /union officers and other stakeholders may not. Breaches involving encrypted data are not exempted from the notification and reporting requirements of PIPEDA.

The use of high-quality encryption may reduce the risk of harm to below the **real risk of significant harm** threshold so no notification or reporting would be required. In such circumstances, the Plan must maintain a record of the breach for 24 months.