Privacy

The federal government of Canada requires all organizations and companies that gather client information to be subject to certain guidelines of the Personal Information and Electronic documents Act (PIPEDA). The act's guidelines are summarized in the 7 points of the Client brochure as seen below.

Queen Financial Group Inc.(QFGI) follows established federal government guidelines of the Personal Information Privacy and Electronic Documents Act (PIPEDA). PIPEDA sets out regulations to organizations for the collection, use and disclosure of personal information in the course of commercial activities.

QFGI recognizes an individual's right to privacy and adheres to the following principles when using personal information for legitimate business purposes. The regulations pertain to officers, employees, agents, sales representatives and administration personnel of QFGI.

- QFGI and its personnel are responsible for protecting client personal information in possession or custody whether in electronic or paper-based format.

- QFGI maintains strict security systems to safeguard any personal information in storage or in the event of disposal of unneeded data.

- Client personal information provided to QFGI in the course of business purposes can be verified with government agencies and other fact collecting entities.

- QFGI requires a contractual arrangement that is consistent with GFGI measures with any person or organization providing essential third-party business related services.
- Any client personal information proposed for use that is deemed not necessary to the usual course of business will require prior consent of the client.
- Client personal information will be kept and disclosed to meet legal regulations of government authorities and for special circumstances, such as fraud investigations, or other situations permitted by law.
- The Privacy Officer of QFGI is available to be contacted at 416-848-0288 with regards to the QFGI privacy policy, to handle complaints in cases of breach of privacy and to resolve related issues. A client who has provided

personal information has the right to review the information. Concerns not resolved to your satisfaction can be furthered to the Office of the Privacy Commissioner of Canada or, if applicable, the Provincial Privacy Commissioner.

The above brochure is available to every client of QFGI . When involved with sensitive client data it is our duty as employees of the various departments of QFGI to make sure that policy is enforced with practices that ensure the confidentiality of the data.

PIPEDA requires organizations to protect personal information, establish procedures to receive complaints and inquiries, make staff aware of company policies through training and other means, and develop information to explain the organization's policies and procedures.

Some more specific considerations for our organization are as follows:

Purpose

Purposes for gathering client data information must be identified and made known with client consent at the time of collection. The consent applies to material that is considered as sensitive. There are exceptions for information use without consent and they must be justified. There are different ways of gaining consent including application, check off box, orally over the phone, and use of service or product.

New purposes for information use require documentation, identification and client consent prior to use.

Protecting Client Personal Data

Protection measures include: physical – locking filing cabinets and restricting access to certain areas and offices, organizational measures dealing with security clearance limiting access, technological measures like passwords and encryption. More sensitive material is to be safeguarded at higher security levels as appropriate.

Third Party Use

Third parties that are contracted to perform services for the original organization having custody of client personal data must have policies in place that the information supplying organization has approved and agreements are recommended that the PIPEDA will be followed to mutual satisfaction.

Retention and Disposal

Personal information should be only retained for as long as necessary to fulfill the purpose. Disposal of personal information must be done in a confidential manner.

Personal information no longer required should be destroyed erased or made anonymous. Guidelines to deal with unneeded client data should be implemented.

Disclosure to Clients and Openness

A policy complete with method and procedures should be made available to clients regarding privacy and the practices used to maintain it. The information disclosing privacy practices is to be openly available to the public to a reasonable extent dependent on the medium and the message.

Access to Personal Information

Individual client access to information includes: a person or group that is responsible and accountable for the organization's policies and practices, the means of gaining access to personal information held by the organization, description of the information held and a general account of its use, a copy of a brochure or info that explains the organization's standards and policies, and what personal information is made available to related organizations.

An individual can access their own personal information upon request and can challenge, complete and can cause information to be amended for accuracy. A company is obligated to change records when proven incorrect. Accuracy in completeness and being up to date on data is a necessary function of the organization.

Exceptions for supplying personal information to a client can be limited in certain circumstances as to reasons of cost, retrieval difficulties etc. that are backed with an explanation. An individual's request for information should be made on a timely and minimal or no cost basis.

10 Steps	Representative's Role	QFGI 's Role	Go Forward
Accountability	Become familiar with the ten steps and how they affect your daily work. Incorporate QFGI 's policies, procedures and practices to	To assist the representative in understanding the privacy legislation and QFGI 's policies. Assist the representatives in	Amend existing policies and procedures and monitor every person's compliance with QFGI 's ten steps.

	protect clients' information into everyday activities.	putting these policies into practice.	
Providing Purpose (Informing clients of the reason(s) for collecting their information, before or at the time of collection).	Every representative must clearly explain to each client why their personal information is collected and how it will be used. Information collected should be limited to the original purpose for which it was collected, and should be enough information to: 1. Understand the client needs 2. Provide ongoing service 3. Establish and maintain communication with the client	Use client information to provide products and services. Compile statistics to help understand the needs of the clients.	Purpose is identified on all applications – "Privacy Policy" QGFI must ensure that full disclosure is made at the time of collection.
Consent: Client knowledge and consent is required before information is collected, used, or disclosed.	Every representative must ask for client consent when collecting personal information. Every representative must record how the client's consent was received.	Ensure that proper consent is received before disclosing information to an authorized individual.	QGFI cannot and will not disclose any information until we have ensured that consent has been given. A consent to disclose note can be added to a client file – with the name of the person to whom consent has been granted.
Limiting Collection of Personal Information	Every representative must ensure that client information is not collected indiscriminately and that the source of the information has been verified. Whenever possible, every representative should obtain	Collect only information necessary for the legitimate purposes identified.	QGFI must ensure that client information is not collected indiscriminately and that the source of the information has been verified. Compliance professionals and Branch

	the information directly from the individual concerned.		Managers will be utilized to monitor this step.
Limiting Use, Disclosure and Retention	Client information will not be used or disclosed in any other way except for that which it was originally collected.	QGFI will only provide information of potential clients (“prospects”) to QGFI representatives, only if these prospects have provided prior consent. QGFI will not provide sales representatives with existing client information - unless it is to fulfill the identified purpose. QGFI will destroy, erase, or make anonymous any client information that is no longer required to fulfill the identified purpose.	QGFI will ensure that client information will not be used or disclosed in any other way except for that which it was originally collected.
Accuracy	Client information should be recorded carefully and accurately. Changes to client information should be verified with the client.	Customer service must ensure that every representative records clients’ information carefully and accurately.	QGFI will include in its policies that no changes will be made to client files without the information first being verified with the client – once this has been confirmed, QGFI will ensure that changes

		Changes to client information should be verified with the client.	
Safeguarding Clients Personal Information	All sales representatives must properly secure all personal information received by a client (paper or electronic copies) against loss, theft or unauthorized access. There should be procedures in place for working mobile/offsite to protect client information outside of QGFI's premises.	QGFI has made reasonable efforts to protect client information regardless of the format. The level of security is appropriate to the level of sensitivity of the information.	QGFI will enhance its practices. Physical measures will include: locking desk drawers, filing cabinets; restricting access to offices. Technological measures includes: using more passwords; encryption, and firewalls.
Client Access	All sales representatives must ensure that clients are aware of QGFI's privacy policies and practices as well as the management and storage of their personal information.	QGFI informs clients within 30 days after a written request about the existence, use, and disclosure of personal information and gives them access to it.	QGFI will ensure that clients are more aware that they have access to their personal information. In addition Global will inform client's that they can challenge the accuracy and completeness of the information and have it amended.
Openness	All sales representatives must be aware of aware of QGFI 's privacy policies and practices.	QGFI has made its information about its policies and procedures readily available to clients.	QGFI must conduct regular training of its privacy policies and the management of client information.
Handling Client Complaints	Clients should be made aware of a complaint process; it should be simple and easily available.	QGFI has procedures in place to receive and respond to	QGFI must hone its complaints process and address client concerns and questions as quickly as

and Questions	All complaints received should be investigated. Steps should be taken to correct practices after the outcome of a complaint.	compliments or complaints relating to the handling of client information. QGFI investigates all complaints – and if well founded, Global takes appropriate measures, including amending policies and procedures if necessary.	possible. QGFI must make changes and amend policies and procedures if necessary.

Privacy Breach Protocol

The following five steps will be initiated as soon as a privacy breach, or suspected breach, has been reported. The Privacy Officer will document the breach and guide the manager (employee or sales person) through the breach management process.

Step 1 – Report. Report and assess the report upon becoming aware of a possible breach of personal or confidential information. The suspected breach must be promptly reported to the Privacy Officer. This shall occur even if the breach is suspected and not yet confirmed. The report should capture:

1. What happened?
2. Where did it occur?
3. When did the suspected incident occur?
4. How was the potential breach discovered?
5. What kind of information was breached e.g.: technology, paper files, shared through people?
6. Was any corrective action taken when the possible breach was discovered?

Step 2 – Containment. This involves taking immediate corrective action to put an end to the unauthorized practice that lead to a breach. The main goal is to alleviate any consequences for both the individual(s) whose personal or

confidential information was involved and QGFI. All containment activities or attempts to contain the privacy breach shall be documented by the Privacy Officer.

Step 3 – Investigate. Once the privacy breach is confirmed and contained, the Privacy Officer shall conduct an investigation to determine the cause and extent of the breach by:

1. Identifying and analyzing the events that led to the privacy breach. Did QGFI take reasonable precautions to prevent the breach?
2. Evaluating if the beach was an isolated incident or if there is risk of further privacy breaches. Revised Aug 2016
3. Determining who was affected by the breach e.g. clients or personnel, and how many individuals were affected.
4. Evaluating the effect of containment activities.
5. Evaluating who had access to the information.
6. Evaluating if the information was lost or stolen.
7. Evaluating if the personal or confidential information has been recovered.

Step 4 – Notify. Notification includes notification to the affected individual(s), authorities and/or other organizations (like the police if identity theft or other crimes are suspected). Affected individuals will be promptly notified and receive the initial notification as soon as possible after the breach has occurred. Further communication with the affected individuals may occur during the process as updates occur. The method of notification shall be guided by the nature and scope of the breach and in a manner that is reasonable to ensure that the affected individual will receive it. Direct notification e.g. by phone, letter, email or in person shall be used where the individuals are identified.

Step 5 – Prevention of Future Breaches. Once the breach has been resolved, the Privacy Officer, Management and the Executive of QGFI will work with the together to develop a prevention plan or take corrective actions as required. Prevention activities might include: audits; review of policies, procedures and practices; employee training; or a review of service delivery.