INTERNAL PRIVACY and BREACH POLICY
Full Circle Financial Inc.

Objective
To ensure that:

(a) I am in compliance with regulatory and self-regulatory requirements regarding Privacy ("Regulations");
(b) A client's Privacy is handled in a professional manner, in a secure environment and appropriately monitored;

The Privacy Officer
Person Responsible is **Kevin Giffin**

(1) I, **Kevin Giffin** am the Privacy Officer and all inquiries/complaints shall be directed to me
(2) I, **Kevin Giffin** am hereby designated as responsible for the application of this policy;

My Commitment
My clients are my business. As an advisor, I am trusted with some of my clients' most sensitive personal information. I must respect that trust and need my clients to be aware of my commitment to protect the information they provide in the course of doing business with me.

I collect personal information in compliance with applicable laws and ethical business practices, in order to provide services and to conduct business. I limit the information that I collect to that which it is necessary for, or related to, these purposes.

I abide by the **Ten Privacy Principles**. The Principles are based on the federal government's privacy legislation, the *Personal Information Protection and Electronic Documents Act*

1. 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.

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

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

4. 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.

5. 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 the law. Personal information shall be retained only as long as necessary for fulfillment of those purposes.

6. 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.

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

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

9. 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.

10. Challenging Compliance: An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals for the organization's compliance.

Information Collection and Use
I collect the information required to complete the task for which I am engaged, whether that is insurance, money products or financial plans.

Personal information is information that refers to you specifically. I will use fair and lawful means to collect your personal information. I will only collect information that is pertinent and consistent with the purposes of the collection. Whenever practical, I will collect the required information directly from the client, or from their authorized representative(s), in completed applications and forms, through other means of correspondence, such as the telephone, mail or the internet, and through their business dealings with me.

What I need to know and why
I collect information from my clients and about them, only with their consent, or as required or permitted by law. In general, I will collect personal information such as their name, address, telephone number(s) or other identifying information, such as their Social Insurance Number (SIN) or date of birth.

The type of additional information that I gather will depend on the type of product or service involved. The information gathered may be financial, which would include such information as place of employment, annual income, assets and liabilities. It may be investment or advice related, requiring information on such things as your financial goals and retirement plans. If the client is applying for insurance or group insurance benefits, it may also include health information or lifestyle related information, such as their occupation, travel history and plans, driving record or criminal record.

Consent
The consent is for me to establish a file and collect and maintain personal, medical & financial information and is to be signed by the client and placed in their file.

Protection of Personal Information
As the advisor, I am granted access to client information and must understand the need to keep the information protected and confidential. My procedures clearly communicate that I am to use the information only for the intended purpose(s).

If I hire a staff member, he/she will be required to sign a confidentiality agreement upon commencement of employment.

Retention of Personal Information
I will only keep client’s personal information in my records for as long as it is needed to fulfill the identified purposes, or as required or permitted by law.

Privacy Choices
Clients may request copies of my privacy policies and procedures at any time.

Clients may request access to their information. I must respond to this request as quickly as possible, but no later than 30 days after the receipt of the request.

Clients may withdraw their consent at any time by contacting me as the Privacy Officer. However, they will be made aware that failure to provide adequate information may prevent me from completing the task for which we were engaged.

Clients may file complaints about my privacy procedures as well as a breach in my privacy policy. Complaints should be received in writing and forwarded to the Privacy Officer. The Privacy Officer will contact the client and obtain all details. The Privacy Officer will then review the circumstances of the complaint and determine if there is reason to alter the existing privacy policy. Insurance carriers should be notified of any complaint involving their clients/products.

Exception to client access

Organizations must refuse an individual access to personal information:

- if it would reveal personal information about another individual unless there is consent or a life-threatening situation
- if the organization has disclosed information to a government institution for law enforcement or national security reasons. Upon request, the government institution may instruct the organization to refuse access or not to reveal that the information has been released. The organization must refuse the request and notify the Privacy Commissioner. The organization cannot inform the individual of the disclosure to the government institution, or that the institution was notified of the request, or that the Privacy Commissioner was notified of the refusal.

Organizations may refuse access to personal information if the information falls under one of the following:

- solicitor-client privilege
- confidential commercial information
- disclosure could harm an individual's life or security
- it was collected without the individual's knowledge or consent to ensure its availability and accuracy, and the collection was required to investigate a breach of an agreement or contravention of a federal or provincial law (the Privacy Commissioner must be notified)
- it was generated in the course of a formal dispute resolution process.

Privacy Breach Policy

Full Circle Financial Inc
Advisor/Company Name)

Contact Information

___**Kevin Giffin**___
(Privacy Officer)

54 Great Oak Dr. Toronto,ON M9A 1N2
(Address)

___416-341-7901___
(Telephone #)

___1-866-363-6036__
(Fax #)
kgiffin@fullcirclefinancial.ca
(Email address)

At ***Full Circle Financial Inc.*** we have a responsibility for the safekeeping and protection of personal information that we collect and retain on our employees & clients.
Part of our responsibility is to document and report any privacy violations/breaches of such personal information.

What is a breach?
A privacy breach is the result of an unauthorized access to, or collection, use or disclosure of personal information.

Why you should notify individuals in certain circumstances
Your customers and employees expect businesses to protect their personal information. They want to be informed about privacy risks associated with your personal information handling practices.

What to do after discovering a breach

- **Complete privacy breach incident form**
  - Complete form in full, include all details

- **Conduct preliminary assessment**
  - Contain breach
  - Designate individual to start investigation
  - Preliminary notification
    - Escalate internally (personal responsible for privacy compliance)

- **Evaluate the risks**
  - what personal information was involved
  - what was the cause and extent of the breach
  - how many individuals have been affected and who are they
  - what harm could result from the breach

- **Notify all appropriate parties**
    - Financial Institution
    - Client
    - Police
    - Privacy Commissioner

- **Prevent future breaches**
    - Review and establish new policies/prodigal/training (if applicable) to prevent future breaches

If anyone has any questions with regards to the information contained within this policy, please contact:

Kevin Giffin
(Privacy Officer)

Checklist for Office Safeguards
(Individual/Corporate Advisor Offices)

Below is a list of safeguards you can implement in your office. This checklist can be customized to fit your office needs.

- Employees to read and acknowledge in writing that they understand and will abide by the privacy policy
- All staff are required to sign a confidentiality agreement
- Privacy disclaimer on all e-mail, faxes etc.
- All confidential materials to be removed from view (during lunch, breaks, end of day)
- No information in view of public, on desks
- No discussion of client files outside the office
- Computers/Laptops to be secured when unattended
- All computers/laptops to be password protected
- No sharing of passwords
- All file cabinets to be locked
- All waste paper containing personal information be shredded
- Any person, client or broker, must identify themselves by a broker code, SIN #, DOB, etc to confirm identity
- No sharing of client information with unauthorized parties
- Fax Machine to be set up to keep faxes in memory when office is closed
- Office is locked and alarms set when no staff present or on weekends
- All privacy related client complaints to be referred to Privacy Officer
- Empty shredding file daily
- Lock shredding bin
- Certificates of Destruction are received for shredded material

All inquiries should be directed to the Privacy Officer:

Kevin Giffin
(Privacy Officer)

Privacy Breach Checklist
(Guidelines & Steps to assist you with reporting)

Incident Description

- When was the date of the incident?
- Who discovered it?
- Details of what happened?

Step 1: Breach Containment and Preliminary Assessment

- Have you contained the breach (recovery of information, computer system shut down, locks changed)?
- Have you designated an appropriate individual to lead the initial investigation?
- Have you determined who needs to be made aware of the incident internally and potentially externally at this preliminary stage?
- Does the breach appear to involve theft or other criminal activity? If yes, have the police been notified?

Step 2: Evaluate the Risks Associated with the Breach

(i) What personal information was involved?

- What personal information was involved (name, address, SIN, financial, medical)?
- What form was it in (e.g., paper records, electronic database)?
- What physical or technical security measures were in place at the time of the incident (locks, alarm systems, encryption, passwords, etc.)?

(ii) What was the cause and extent of the breach?

- Is there a risk of ongoing breaches or further exposure of the information?
- Can the personal information be used for fraudulent or other purposes?
- Was the information lost or was it stolen? If it was stolen, can it be determined whether the information was the target of the theft or not?
- Has the personal information been recovered?
- Is this an isolated incident?

(iii) Who has been affected by the breach (employees, clients, service providers, other organizations)?

(iv) Is there any foreseeable harm from the breach?

- What harm to the individuals could result from the breach (e.g., security risk, identity theft, financial loss, loss of business or employment opportunities, physical harm, humiliation, damage to reputation, etc.)?
- Do you know who has received the information and what is the risk of further access, use or disclosure?
- What harm to the organization could result from the breach (e.g., loss of trust, loss of assets, financial exposure, legal proceedings, etc.)
- What harm could come to the public as a result of notification of the breach (e.g., risk to public health or risk to public safety)?

Step 3: Notification

(i) Should affected individuals be notified?

- What are the reasonable expectations of the individuals concerned?
- What is the risk of harm to the individual? Is there a reasonable risk of identity theft or fraud?
- Is there a risk of physical harm? Is there a risk of humiliation or damage to the individual's reputation?
- What are the legal and contractual obligations of the organization?
- If you decide that affected individuals do not need to be notified, note your reasons.

(ii) If affected individuals are to be notified, when and who will notify them?

- What form of notification will you use (e.g., by phone, letter, email or in person, website, media, etc.)?
- Who will notify the affected individuals? Do you need to involve another party?
- If law enforcement authorities are involved, does notification need to be delayed to ensure that the investigation is not compromised?

(iii) What & Who should be included in the notification?

Depending on the circumstances, notifications could include some of the following, but be careful to limit the amount of personal information disclosed in the notification to what is necessary:

- a description of the personal information involved in the breach;
- contact information in your organization who can answer questions or provide further information;
- whether your organization has notified a privacy commissioner's office;
- Should any privacy commissioners' office be informed?
- Should the police or any other parties be informed? This may include insurers; professional or other regulatory bodies; credit card companies, financial institutions or credit reporting agencies; other internal or external parties such as third-party contractors, internal business units not previously advised of the privacy breach

Step 4: Prevention of Future Breaches

- What short or long-term steps do you need to take to correct the situation (e.g., staff training, policy review or development, audit)?

Privacy Breach Incident/Reporting Form

Date:	
Name of Individual completing form	
Location & date of incident	
Description of incident	
Cause (if known)	
Effected individual(s) (client, employee, advisor, 3rd party)	
Type(s) of personal information involved	
Brief description of action(s) taken to contain breach	
Who has been notified (including date notified)	
Additional Comments	

Staff - Privacy Training

Training sessions and meetings:

Date	Topic	Employee Name

Privacy Policy Review Log

Review Date	Item updated	Reviewer Name and Title