COMPLIANCE PROGRAM FOR PRIVACY

Required under Personal information protection and electronic documents Act (PIPEDA) or applicable provincial privacy legislation

Healy Financial Planning

Compliance Officer: Tracey Feenstra

Effective: May 30, 2014
Revised on:

Table of Contents

Appointment of a Compliance officer/Resolution of the board (to be included for incorporated advisors only, delete if sole proprietor)

RESOLUTIONS OF THE BOARD OF DIRECTORS OF
[Healy Financial Planning] (The "Firm")
EFFECTIVE [May 30, 2014]

WHEREAS the Firm must adopt a compliance program in order to comply with PIPEDA (the "Act") and/or applicable provincial legislation, applicable to its operations;

WHEREAS the Firm must ensure that persons that it hires and/or who act on its behalf, whether or not they have a sales licence, comply with the same provisions;

WHEREAS in order to ensure compliance with the various applicable rules, the Firm wishes to adopt a compliance program and to appoint one or more persons to be responsible for the application of this program;

IT IS THEREFORE RESOLVED:

THAT the compliance program attached is hereby adopted by the Firm;

- **THAT** [Tracey Feenstra] is/are appointed as compliance officer(s) with regard to the Act;

THAT as compliance officer(s) [Tracey Feenstra] is responsible for:

- Implementation and monitoring of the compliance program;
- Establishing and periodically revising the Firm's policies and procedures;
- Initial and continuing training of representatives, employees and persons acting for and on behalf of the Firm;
- Immediately notifying the principal of the Firm of any known or presumed violation of the Firm's compliance program;

THAT the compliance officer(s) may obtain the assistance of another person to manage the Firm's compliance responsibilities provided that this person has the requisite experience and skills in respect of the compliance aspects that are entrusted to him or her, provided that the name of this person or these persons and his/her/their responsibilities are documented in the compliance program.

THAT [Matthew Healy] is authorized to sign documents and take any other measures required to give full effect to the resolutions herein.

The resolutions herein are adopted by the director(s) of the Firm as witnessed by his/her/their signature(s) below.

_____ _____

Signature Date

ACCEPTED BY THE COMPLIANCE OFFICER(S):

_____ _____

Signature Date

Section 1- Reviews and amendments to the compliance program for privacy

This program was adopted on: May 30, 2014

Document revision history

Date	What changed?	Reason for the change

Section 2 - Self-review

Date of review: May 30, 2014

Name of person completing review: Tracey Feenstra

Signature of principal/advisor: _____

Accountability	Yes	No	Comments
I/We have designated a person to oversee compliance with privacy legislation and know that the name of the designated person must be made available to a client on request.	X		Tracey Feenstra
I/We have implemented procedures to protect personal information.	X		See privacy compliance binder
I/We have communicated and trained staff about policies and practices.	X		We have had 0% turnover in over 5 years
I/We understand that personal information should not be collected that is not needed to fulfill the purpose identified.	X		Only obtain info required to do financial planning.
I/We understand that when providing third parties (e.g. computer consultants, cleaning staff, accountants, etc.) access to personal information, I/we must have contractual or other means to provide a comparable level of protection.	X		Generally confidentiality agreement built into third party contracts. On the occasion this not the case we …
I/We am/are aware and follow London Life's Privacy Guidelines and strong business practices.	X		Sign code of conduct every year and review information.
I/We understand London Life's process regarding privacy complaints and inquiries.			Sign code of conduct every year and review information.
Consent	**Yes**	**No**	**Comments**
I/We understand that I/we am/are responsible for obtaining consent for the collection, use and disclosure of personal information.	X		Client signs consent form we provide.
I/We have a process in place to obtain consent from clients for the collection, use and disclosure of their personal information.	X		Every new client and new sale.
My/Our process makes a reasonable effort to tell the client how his/her information will be used or disclosed.	X		Explained in every interview and application.
I/We understand that the form of consent used must reflect the sensitivity of the information collected.	X		
I/We understand that consent must be given by the client or by an authorized representative (e.g. legal guardian, general power of attorney).	X		
I/We have a process in place to manage opt-out and withdrawal of consent (e.g. can track and respect the wishes of clients who have opted-out)	X		

Limiting collection	Yes	No	Comments
I/We only collect information that is necessary to fulfill the purpose(s) disclosed to the client.	X		Limit collection of information to provide financial planning and ongoing service related to the products sold.
The information is collected by fair and lawful means.			
Limiting use, disclosure and retention	**Yes**	**No**	**Comments**
I/We understand that if personal information is intended to be used for a new purpose I must disclose that purpose to the client and obtain his/her consent.	X		Review in every client interview.
I/We have guidelines and procedures for the retention of personal information.	X		Follow London Life's retention guidelines.
I/We have taken steps to ensure that when disposing of or destroying personal information, unauthorized parties will not access it.	X		Shredder available in our office.
Accuracy	**Yes**	**No**	**Comments**
I/We have a process in place to ensure that the personal information collected and used is as accurate, complete, and up-to-date as is necessary for the purpose(s) for which it is to be used.	X		Verify at each transaction.
Safeguards	**Yes**	**No**	**Comments**
I/We have security safeguards in place to protect against loss or theft, as well as unauthorized access, disclosure, copying, use or modification of personal information.	X		See section 3 policies and procedures section Safeguards
I/We use a higher level of protection for sensitive information. My/Our methods of protection include: • Physical measures (e.g. locking filing cabinets, restricted access to office, etc.) • Organization measures (e.g. limiting access on a 'need-to-know' basis) • Technological measures (e.g. use of passwords and encryption)	X		See section 3 policies and procedures section Safeguards
I/We have made employees aware of the importance of maintaining the confidentiality of personal information	X		See section 3 policies and procedures section Safeguards
Openness	**Yes**	**No**	**Comments**
Clients can easily obtain information about my privacy policies and practices.	X		As stated on our website
Individual access	**Yes**	**No**	**Comments**
I/We understand that clients have a right to request information about them held in files I maintain.	**X**		
I/We have a process in place if a client requests access to/her personal information.	**X**		Requested are handled by our compliance

			officer for information we have on file.
I/We understand that clients have a right to request information about them held in files maintained by London Life.	X		
I/We know what London Life's process is if a client requests access to his/her personal information held at London Life.	X		Requested are handled by our compliance officer for information held by London Life. See section 3 policies and procedures for provider contact information.
Actions required:			

Section 3 - Policies & Procedures

Table of Contents

1. Privacy and your business

Clients provide me/us with personal information that is essential to my/our business and protecting this information is important to maintaining their trust and confidence. The federal privacy law, the Personal Information Protection and Electronic Documents Act (PIPEDA), governs the collection, use and disclosure of personal information. Personal information is defined as any information about an identifiable person (including health and financial information), with the exception of the person's name, business address and business phone number where the person is an employee of an organization.

I am/We are responsible for taking appropriate steps to safeguard the personal and confidential information in my/our possession. In some situations, this will mean I/We must adopt new business practices to safeguard personal information.

I/We abide by London Life's privacy guidelines, which are based on principles recognized in PIPEDA.

2. Concerns and general requests

Any concerns or general requests related to privacy and my/our practice will be addressed with the client as soon as possible and no later than 48 hours from the request or if I'm/We are away no later than 48 hours after my/our return.

Any concerns or general requests related to privacy and London Life products and services are to be made in writing and sent to:

London Life Insurance Company:

Chief Compliance Officer
London Life Insurance Company
255 Dufferin Avenue
London, ON
N6A 4K1

The Chief Compliance Officer can also be reached by e-mail at chief.compliance.officer@londonlife.com.

Client requests for personal information

Under PIPEDA, clients have the right to request information about them held in files maintained by either me or London Life.

Any client requests for access to personal information held in client files will be addressed within 48 hours. The client has the option of receiving a copy mailed to their home address or access in person through a scheduled meeting in my office.

Contact the Ombuds' office at ombudsman@londonlife.com or by calling 1-866-292-7825, if a client requests access to his/her personal information held with London Life. See Appendix B – Process for handling privacy concerns for more information on this process. All advisors and employees are required to be aware of this process and must be able to provide direction to clients when requested.

Misuse of personal information:
All reports of misuse of personal information must be reported to the compliance officer and the compliance officer will report as required.

Any misuse of personal information relating to London Life products and services should be reported immediately to the chief compliance officer at chief.compliance.officer@londonlife.comcommunications.

3. Collection of personal information:

I/We only collect personal information that is necessary for the purposes identified.

I/We take reasonable efforts to ensure client and prospect information held in client files is accurate and is updated or corrected as needed.

I/We take appropriate measures to ensure that information I've/we've collected is used for the purposes identified and that it is not used for another purpose or disclosed to a third party without the client's or prospect's consent, except as may otherwise be allowed by law. Procedures to determine appropriateness of a third-party service provider to store, process or manipulate client personal information and safeguards used by that third party are outlined in Appendix C.

I/We follow London Life's client file policy and guideline which describes what to keep in a client file and use the client file authorization form both of which can be found on the Advisor Site under Resources > Compliance and guidelines > Client file & record retention.

Recording client telephone calls

Any recording of client calls involves the collection of personal information therefore the practice must meet fair information practices. The same rules apply to calls initiated by the client and to calls initiated by the advisor.

- I/We may only record calls for specified purposes;
- The individual must be informed that the conversation is being recorded at the beginning of the call and I/we must make a reasonable effort to ensure the individual is advised as to the purposes for which the information will be used;
- Recording may only take place with the individual's consent. If the caller objects to the recording, I/we should provide the caller with meaningful alternatives;
- The information collected must only be used for the specified purposes; and
- I/we must ensure that I/we comply with the other provisions of the Act with respect to matters such as safeguards, access, retention and disposal.
- If a client requests access to their information in my/our files, it is conceivable that I/we will have to provide the recording or transcription of the recording of calls with the client.

4. Use, disclosure and retention:

Personal information that is no longer required to fulfill the purpose(s) identified when it was collected is destroyed or erased. If I/we believe I/we have a need to keep any additional information I/we have the client sign the appropriate area of the authorization form allowing me/us to retain this material.

I/we am solely responsible for the safe keeping of this material, for maintaining its confidentiality and for its return to the client.

When paper materials containing any client or prospect personal information are to be destroyed, this should be done by shredding, not recycling.

I follow London Life's record retention guidelines for information related to London Life business found on the Advisor Site under Resources > Compliance and guidelines > Client file & record retention.

5. Safeguards

Appropriate safeguards must be taken in the storage and disposal of client information. I/We use encryption software on all electronic devices. When information is no longer required I/we dispose of client information by shredding paper and ensuring all information has been deleted from end user devices including personal computer (desktop or laptop), consumer device (e.g., personal digital assistant (PDA), smart phone), or removable storage media (e.g., USB flash drive, memory card, external hard drive, writeable CD or DVD) that can store information. Storage devices must destroyed when being disposed of to ensure the information is not retrievable.

I/We take appropriate precautions to safeguard client information from third parties who may have access to the premises, i.e., security, cleaning services and suppliers.

See Appendix D – Safeguards for additional information for safeguarding personal information.

6. Consent

When collecting information from clients and prospects, I/we must be prepared to explain the purposes behind why I am/we are collecting this information. While client consent to our collection and use of personal information does not necessarily need to be stated directly or in writing, I/we provide information to a client or prospect about my/our own privacy practices – see Appendix E My Commitment to Protecting Your Privacy. This information can be given verbally to clients or provided on paper at an initial meeting. In keeping with good client file practices, I/we document in the client's file that this information was reviewed with the client or prospect.

I/we only disclose personal information about clients to another person or company if I/we have the verbal or written consent of the client, or if I am/we are otherwise allowed or required to do so by law. I/We can recommend other professionals or advisors to clients if they ask me or if I/we believe they may benefit from such services. I/We never provide any client names or other information to third parties who may use it to market their services unless I/we have the client's consent.

Steps to obtaining client consent

- I/We obtain consent from all clients for new access to their information. This includes sales of business to another advisor or providing access to a new administrative support person (excluding London Life employees). The consent requirement can be handled a number of ways - by telephone, fax, email, letter, newsletter or a personal visit. I/We send a letter.
- The letter should name the new advisor and contain a contact name and number for the current advisor, in case the client, on receiving the letter, objects to the transfer of his or her information or to its access by another advisor.
- If a client objects to this transfer or new access, depending on the situation, the client has the right to:
    - Request that his/her information not be disclosed to the new advisor
    - Request a new advisor
    - Receive the names of other advisors to contact or be provided with the name and number of the regional director, or vice-president where they can request another advisor
- The new advisor should not use or access information in the client file until consent is obtained. I/We recommend allowing 10 to 20 business days for the client to voice an objection, after which time it can be assumed consent has been obtained.
- The new advisor is responsible for handling the file/information appropriately going forward.

Temporary access to a client's information – a short-term or temporary absence from my practice

If I am/we are not able to provide service to clients for an extended period of time and I/we seek help from another advisor or new administrative support person, I/we obtain consent(s) from client(s) to allow servicing of the business by another advisor or new administrative person (and therefore access by a new person to their records). The process to obtain these consents is the same as that described above under *Steps to obtaining client consents*.

Buy/sell agreements

The selling advisor should protect client information during the valuation process or when seeking a buyer for the book of business. While there may be other suitable methods to accomplish this, I/we:

- Block out identifying client information on documents shared with third parties, or contact our legal counsel to draft a suitable confidentiality agreement that should be signed by third parties involved in the process of valuing the book for potential sale.
- As outlined above, in Steps to obtaining client consent, the selling advisor should obtain client consent to the transfer of his/her information prior to the completion of the sale.

Agent of Record (AOR) changes

Since clients initiate AOR transfers, I/we can assume that I/we have implied consent to transfer access to their information and their files (or a copy of their files), if applicable to the new advisor. Therefore, there's no need to have official consent included along with instructions from the client.

Appendix A – Undertakings of employees and advisors of (Healy Financial Planning)

All employees and advisors are required to read the Policies and Procedures so that they understand the privacy principles.

I,_____ , confirm having read the Compliance guide for privacy of (Healy Financial Planning) and related procedures, and undertake to comply therewith.

SIGNED AT _____ ON _____.

_____

Name:

_____

Title:

Appendix B – Process for handling privacy concerns

Definition of a Privacy Complaint:

Any concern relating to a privacy issue, whether through an individual or a third party venue. This could be client information going to the wrong address, (someone else opening the mail) personal information being shared with other parties, release of personal information without proper authorization, or use of personal information without proper consent.

What is proper authorization?

Proper authorization is where the policyowner has provided written instructions that I/we can release information about their insurance product to another individual. Ensure that the consent, purpose and use are appropriate for the authorization.

Verbal authorization may be accepted as long as proper authentication has been completed on the policyowner.

When to refer a privacy concern related to London Life products or services to the ombudsman:

The ombudsman can be reached at 1-866-292-7825 or emailed at ombudsman@londonlife.com .

All concerns where an individual's personal information has been released without their consent

- Email scams
- Email solicitation
- Laptop or any other data security
- All escalated privacy concerns – client requests to speak to senior management level
- All concerns, relating to privacy, where the client is very upset - transfer the call directly to ombudsman, or indicate that I/we will call client back as soon as possible
- Concerns where client remains dissatisfied with the business area's decision.

NOTE: It is important that any privacy complaint, received in a business area, be reviewed as quickly as possible and if necessary, sent to the ombudsman. I/we must investigate and respond within 30 days of receipt of complaint.

Access or change of information on a London Life client file:

Any requests for access or to change information on a client file must be referred directly to the ombudsman.

Routine document requests, such as copies of title forms, etc. are to be handled through the business area.

Privacy concerns to be handled in the business area:

- All concerns that can be handled within the normal business area's resolution process (one and done type complaints). For example, two different policyowner's anniversary statements mailed in one envelope.

Process for handling privacy concerns:

- All privacy concerns must be acknowledged within 24 hours of receipt of concern
- All privacy concerns, handled by the business area, must be responded to within 30 days of receipt of concern
- Copy of business area's response must be reviewed by the ombudsman, prior to being sent to client
- Business area provides a copy of the privacy concern documentation to the ombudsman.

Appendix C – Third-party service provider

If a third-party service provider is being used to store, process or manipulate client personal information, the safeguards used by that third party must be carefully considered.

Third-party vendor to store client information:

- **Web-based platform:** I/We will provide London Life's Market Conduct department with the name and contact information for any third party I/we use to store, process or manipulate personal client information. In addition, I/we will let Market Conduct know immediately of any material change of information concerning the third party, or any change involving a new third party. This could mean a switch to a new provider or if a current provider experiences any problems that in turn could affect the security of client information. Providing Market Conduct with this information will also help investigate any impact on me should a provider have any type of security breach or issue.
- I/We will advise the London Life chief compliance officer immediately of any actual or suspected security breach, whether it pertains to my operations or those of a contracted third party. This will allow London Life to determine appropriate action for me or for itself to take in response to a privacy breach involving client information. I/We can reach the chief compliance officer by email: chief.compliance.officer@londonlife.com.

Below are some questions that may help when deciding if using a third-party provider is right for me, and if that provider has the proper safeguards in place for client information. Even if I'm/we are already using a third-party provider I/we should re-visit my provider's processes and safeguards. If these safeguards are not observed satisfactorily I/we should not use the service.

- How long has the provider been in business? A new provider may not have a sufficient track record to allow me to judge its processes and procedures as they relate to the safeguarding of information.
- Can I/we obtain references to assess reputation? References from current users can help me/us gauge the provider's reputation.
- What is their experience in handling sensitive personal and financial information?
- Does the provider have a documented privacy policy in accordance with privacy legislation?
- Do they have a documented and current physical security policy or information security policy?
- Does the provider hold data outside of Canada? Information held in other countries may not have the same safeguards as in Canada and may not be in compliance with my privacy requirements. I/we should make every attempt to use a provider that stores information in Canada or I/we should notify clients that their information will be stored outside of Canada.
- Does the provider have backup and recovery processes? Will I/we be able to access my/our files if the provider shuts down? What will I/we do if the provider loses the client files? Do I/we have a backup?
- Does the provider agree to notify me within 48 hours or less if they incur a data security breach that may involve clients' information?
- If a security breach is suspected, is there support from the provider for an investigation? Are access logs maintained and provided on demand?
- How do I/we back out of or terminate my/our agreement with the provider and ensure data is purged or returned? A provider that does not remove or return information may present a risk to a client's information and therefore to me.

Many of the questions in this guide may be answered in the provider's Licensing Agreement and it must be reviewed carefully. It's a contract, and by clicking "I agree" or by downloading any software, I/we may inadvertently be exposing information I/we store at the site to undue risk if the proper safeguards of information are not adhered to.

There must not be any involvement of any other third parties and/or data sharing, data pooling, or access rights to clients' sensitive information being granted by the service provider. This must be explicitly mentioned in the service provider's agreement.

I/We need to:

- Confirm with the provider that the data they store, as well as data in transmission, is encrypted.
- Understand the limitations of the service provider's liability.
- Check with our legal counsel before agreeing to the terms of the provider. If I/we decide to agree with the provider's terms, I/we should have a printed copy of the agreement for my/our records.

Appendix D – Safeguards

Desks and files:

Sensitive personal information or other client documentation should not be left unattended. Although I/we may need to keep some personal information accessible on my/our desks in paper format for active business purposes, all files and file contents should be placed so that the contents are protected from the view of those without authorization to see them.

I/We must ensure that all sensitive personal information is secured in locked rooms, cabinets and/or desk drawers when not actively in use, and that access is appropriately restricted.

Access to files (physical, system and electronic) should be limited to those requiring access for the performance of their jobs. Access to files must be reviewed when associates/staff are hired, terminated or moved to a different job function.

Office design:

Desks/workspaces are arranged out of the traffic flow within the office. Where possible, I/we locate associates/staff dealing with sensitive client information in an area where conversations will not be easily overheard.

Documents outside of business premises:

I/We must safeguard client information whether in my personal office, car or other location. Paper files containing personal information should be removed from the office only when necessary or required to appropriately service clients.

I/We have documented procedures covering security in respect of files containing personal information that are removed from my/our place of business including effective controls to track removed files. All associates/staff should be aware of the requirements and comply with them.

Computers, consumer devices:

Computers and consumer devices (and if applicable our associate's/staff's computers) are stored securely to prevent access during all absences (evenings, weekends, illnesses, and vacations). I/We use locking cables.

Securing laptops

In the office during the day – Laptops are locked using a locking cable and securely anchored to an immovable piece of furniture or a secure docking station and the lock key is stored in a safe place away from the laptop.

When leaving work at the end of the business day – Laptops are stored in a locked cabinet or drawer, and the lock key is stored in a safe place away from the laptop.

Laptop security rules above still apply when office doors are locked:

On the road:

- While working, position laptops so only the user can see the personal information on the screen.
- Record laptop's serial and model number and keep it in a separate location.
- Carry laptops in a discrete bag. Use a padded bag, such as a backpack, instead of the normal laptop tote, to securely and safely transport disguised laptop.
- Keep laptops out of sight by storing in car's locked compartment during travel to prevent smash and grabs. Never place laptops in a taxi or limousine trunk since most do not lock their trunks.
- Never check laptops with hotels or airlines.
- In airports, after placing laptop on the x-ray conveyer belt, watch the bag and don't let anyone cut ahead.
- At home or in a hotel room, secure laptops as done at work. Bring along the locking cable and lock the laptop down and store it out of sight.
- Card-access hotel rooms produce an accurate audit trail of who has visited the room and when. Metal keys can be lost and copied. If the hotel room uses metal keys, consider not leaving the laptop in the hotel room.

Encryption, screen savers and passwords:

- Use encryption software and always ‘shut down’ (power off) properly. Encryption is not activated if shut down isn’t completed correctly. Encryption does not eliminate the needs for strong passwords.
- Use screen savers or other means to cover personal information on computer screens when others are in the office or work area.
- Secure screen savers should be in place and password protected to prevent unauthorized access.

    - Use combinations of numbers or upper case and lower case letters (e.g. ABDxyz)
    - First letter from each word of a poem, phrase or lyric (e.g. out to lunch > out2lunch, tea for two > teeh42)
    - Special characters like @$%&# whenever possible (e.g. red rose > r3DRO$e!)
    - Avoid using proper names and words found in dictionaries (e.g. insurance, password).
    - Personal information, like family and pet names, birthdays, government ID numbers, or words associated with hobbies and interests.
    - Never write down passwords or share passwords or logon IDs

Communicating confidential information with others:

Voicemail:

Messages left for clients should not contain personal information unless the client is informed in advance that the message may contain personal information and has confirmed that he/she wants this information to be provided on his/her voice message service.

I/We take appropriate measures to authenticate the identity of the person asking for confidential information before it's released. Authentication procedures are provided see Appendix F.

Email:
Messages should not contain personal information unless the client is informed in advance that the message may contain personal information and has confirmed that he/she wants this information to be provided by email.

The following disclaimer is added to all email containing client personal information: "The contents of this communication, including any attachment(s), are confidential and may be privileged. If you are not the intended recipient (or are not receiving this communication on behalf of the intended recipient), please notify the sender immediately and delete or destroy this communication without reading it, and without making, forwarding, or retaining any copy or record of it or its contents. Thank you".

Faxes:
Faxes should not contain personal information unless the client is informed in advance that the fax may contain personal information and has confirmed that he/she wants this information to be provided by fax.

The following disclaimer is added to the cover sheet of all faxes containing client personal information: "The contents of this fax, including any attachment(s), are confidential and may be privileged. If you are not the intended recipient (or are not receiving this fax on behalf of the intended recipient), please notify the sender immediately and delete or destroy this fax without reading it, and without making, forwarding, or retaining any copy or record of it or its contents. Thank you."

Other physical safeguards:
- Fax machines, photocopiers, printers, etc. are located in areas where access is reasonably limited.
- Never discuss clients in public places, such as elevators, cafeterias or restaurants.
- When sharing client or employee personal information on cellular phones, take precautions to avoid being overheard.
- When reading a client's personal information on public transit, such as trains, planes or buses, position documents so as to prevent anyone else from reading it.

Appendix E – My commitment to protecting your privacy

Protecting the privacy of your information is important to me and to the companies whose products and services I offer.

As your financial security advisor, I'll create and maintain a client file for you. This file contains personal information related to you, which I'll gather in order to assess your financial situation, offer you products and provide you with ongoing service. I'll also keep records of our meetings and phone calls, and instructions that you give me in regard to the products and services that you've purchased or might want to purchase through me.

If and when you purchase any product or service through me, you'll complete specific application forms for each. These application forms will request personal information from you that the company offering the product or service requires in order to underwrite or issue the product and provide ongoing services to you and for other purposes as set out on the form. You'll be signing such forms to consent to the use of your information by the company for the purposes indicated on the form. From time to time, you may be required to complete additional forms to confirm your requests for changes in your products or services, or to initiate a claim or benefit. I may keep copies of these forms in your file and the company handling your request may also retain this information.

Your file is kept in my primary place of business. Access to information in your file is limited to me or persons I have authorized to act on my behalf when the information is required for the performance of the person's duties, to the companies I represent in providing, or seeking to provide, products or services to you, to persons you have granted access, and to persons allowed by law.

Signature of advisor: _____

Date: _____

Appendix F – Authentication procedures

If caller is:

- Owner/annuitant
- Joint owners - Single Life Insured/Annuitant
- Joint owners - Joint Insured
- Officer for the company - Corporate owned policy (e.g. President, vice-president, accountant, partner, secretary or life insured's name is the same as the company name)
- Estate of the owner (Person acting on behalf of the estate)
- Owner - In-trust for
- Person or person(s) identified in special handling permitted to receive information
- Power of attorney (and their name is coded on system)

The caller must successfully answer three of the following questions. Always ask the questions in order.

- Full name of owner(s)
- For person calling on behalf of the estate, ask for full name of the deceased owner
- For Owner - In-trust for, ensure the caller's name matches the trustee name on the system
- For power of attorney, caller must provide name of power of attorney in addition to name of policyowner
- Policy number
- Apartment number, street number, street name and city
- Date of birth of the life insured/annuitant
- Full name of life insured/annuitant

Based on response	**Action**
If successful:	Release information.
If validation is not successful:	I am responsible for protecting the privacy and confidentiality of my client's personal information and therefore I cannot disclose any details without first validating that you are the person who should be receiving this information. Please submit your request by mail. -Or- If you check for (missing info)… and call back, I could answer your inquiry by telephone.

If Caller is the payor:

- The caller must provide:
  Full name of the depositor/payor"
  Full name of the owner

The caller must also successfully answer three of the following questions. Always ask the questions in order.

1. Policy number
2. Full name of life insured/annuitant
3. Apartment number, street number, street name and city
4. Date of birth of the life insured/annuitant
5.

Based on response	Action
If successful:	Depositor can suspend banking only. All other requests can be done by policyowner or request sent in writing.
If validation is not successful:	I am responsible for protecting the privacy and confidentiality of my client's personal information and therefore I cannot disclose any details without first validating that you are the person who should be receiving this information. Please submit your request by mail.

For other situations:

Situation	Action
Caller lives with policyowner ✓ Calling to change the policyowner's address	Advise the caller to have the policyowner call back to process the request.
Caller is financial institution ✓ Calling to change banking information or address	Advise the caller to have the policyowner call back in order to process the request
Caller is not the policyowner ✓ Community and Social Services	Give the caller the London Life head office address and ask that they send the form to head office or they can fax it.
Caller is not the policyowner ✓ All other scenarios	I am responsible for protecting the privacy and confidentiality of my client's personal information and therefore I cannot disclose any details without first validating that you are the person who should be receiving this information. Please submit your request by mail.

Section 4 - TRAINING

Training program

Privacy (as per the link on the Learning Center)

Action plan 2013 - 2014

Training material and proofs of training

✓ See attached Certificates of Completion (Privacy Training Module)

Additional information

Included here are emails, brochures or documents relating to our privacy compliance program as well as links to important websites:

Privacy commissioner of Canada: http://www.priv.gc.ca/

Provincial privacy commissions:

Alberta: http://www.oipc.ab.ca/
British Columbia: http://www.oipc.bc.ca/
Provide of Quebec privacy commission/ Commission d'accès à l'information (Privacy): http://www.cai.gouv.qc.ca/index-en.html

The Advisor Site:

Resources > Compliance & guidelines > Privacy, client file & record retention > Compliance program.