THREE LINKS CARE SOCIETY

PRIVACY POLICY

June 2020

TABLE of CONTENTS

PRIVACY POLICY

INTRODUCTION

The Three Links Care Society's privacy policy applies to all Society staff, volunteers, contractors and students. The policy is a consolidation of pre-existing Society policies (**Appendix A).**

In addition to defining accountabilities and key terminology, the policy's scope includes:

- Breach management
- Document retention
- Personal information
- Technology
- Human resources

The policy is supported by other relevant documents and procedure guidelines that are attached to policy (**Appendix B to P**).

Residents registered to use the services of the Society and their designated representatives, individuals employed by the Society, including contractors, volunteers and students consent to the use of their personal information as described in this policy by signing the consent forms in **Appendix K-P**.

PURPOSE

- Protect the privacy and security of residents and their representatives, staff, contractors, volunteers and students.

- Comply with the *Personal Information Protection Act* as a non-profit organization, *Freedom of Information and Protection of Privacy Act* and Vancouver Coastal Health service agreement.

- Exceed compliance requirements where possible to better protect the privacy of residents and their representatives, staff, contractors, volunteers and students.

ACCOUNTABILITY

The Society's Board is responsible for privacy compliance and the delegation of day-to-day accountability to the CEO and Privacy Officer. With approval of the CEO, the Society's Privacy Officer may delegate administrative responsibilities to an appropriate Director or Supervisor in the exercising of their authority under this policy.

The Society maintains a qualified Information Technology consultant to help ensure compliance with this policy, conduct regular system checks and other regulatory requirements.

The Society publishes a *Privacy Statement* on its website and displays it at a prominent location in the Care Centre (**Appendix B**). The Society also publishes a *Whistleblower Policy* that provides protection to employees, contractors, volunteers and students who report a potential contravention of this policy and/or legislation (**Appendix C**). All inquiries should be addressed to:

Privacy Officer, Three Links Care Society
2934 E 22nd Ave, Vancouver, BC V5M 2Y4
E-mail: privacyofficer@threelinks.com

All employees, contractors, volunteers and students of Three Links Care Society shall treat all personal, health and financial information as confidential. Violation of this policy and guidelines may result in disciplinary action up to and including termination of employment or contract.

DEFINITIONS

Confidential Information: All records containing information about the Society that is not generally known, used, or available to the public including but not limited to legal advice, personal, financial, law enforcement and third party business information.

Contact Information: Any information that would enable an individual to be contacted.

Computer Equipment: Any computer hardware owned and operated by Three Links Care Society, including, but not limited to: desktop computers, laptops, tablets, cellphones, printers, copiers, scanners, fax machines and servers.

Computer Network: Electronic information management system, network and mobile devices maintained and operated by the Society to store and manage electronic information collected to carry out duties as an employer and as a health care service provider to the Vancouver Coastal Health Authority.

Designated Representative: an individual, party or organization representing resident's healthcare interest in the event the resident is unable to make a decision. Possible representatives include: a committee of the Person; a representative as appointed by a "Standard" Representation Agreement (no lawyer required, but restrictions as to the authority will apply); a Representative as appointed by an "Enhanced" Representation Agreement (certified by a lawyer), a "Temporary Substitute Decision Maker" (Appointment of a Temporary Substitute Decision Maker form must be completed or a TSDM referral made to the office of the Public Guardian and Trustee).

Indirect Collection: Collection of information from a source other than the individual for whom the information is about.

Information Technology Consultant: Qualified and experienced enterprise retained under a contract to perform services for the Society.

Least Privilege: Principle requiring each subject for a system be granted the most restrictive set of privileges (lowest clearance) needed to perform their employment duties.

Mobile Storage Device: Any portable electronic device that is used to store information, including laptop computers, flash drives, USB drives, external hard drives, smartphones and other similar devices.

Need to Know: Principle where access is restricted to authorized employees and contractors that require it to carry out their work for the Society.

Personal Information: Recorded information about an identifiable individual, including name, home address, telephone number, ethnic origin, sex, marital status, health care history and financial information.

Privacy Breach: Unauthorized access to or collection, use or disclosure of personal information.

Record: Anything recorded or stored by graphic, electronic, mechanical or other means, including books documents, maps, drawing, photographs, letters, vouchers and papers.

Contractor: Person retained under a contract to perform services for the Society.

Three Links Care Centre: 90-bed complex care facility located at the southeast corner of Vancouver's Renfrew and East 22nd Avenue.

Three Links Manor: 39-unit apartment complex across the street from the Care Centre at the corner of Renfrew and East 22nd Avenue.

Two-Factor Authentication (2FA): A security process in which a user provides two authentications to verify the identity of the user in order to protect the user's credentials and the resources they access.

BREACH MANAGEMENT

The Society recognizes privacy breaches can occur when personal information is stolen, lost or mistakenly disclosed. Any employee, contractor, volunteer or student must immediately report a privacy breach in accordance with a *Protocol* developed and maintained by the Society's Privacy Officer (**Appendix D)**.

DOCUMENT RETENTION

The Society's Privacy Officer maintains a document retention schedule to track compliance requirements and achieve policy's purpose. Employees and contractors maintain customized schedules that consider the time required to retain information by law or through contract agreements.

The Society destroys all records containing personal information as soon as retention is no longer necessary for legal or business purposes as prescribed by approved retention schedules. The Society's Privacy Officer develops and maintains procedures to guide these activities (**Appendix E)**.

PERSONAL INFORMATION

Collection and Use of Personal Information

The Society may collect personal information of its residents and resident's healthcare and financial designated representatives as authorized by law to:

- Manage and administer occupant residency at the Three Links Care Centre and Three Links Manor;
- Provide required services or services requested by the resident or their authorized representative - and to assess those services;
- Provide information to third party contractors and medical professionals involved in the resident's care and/or treatment.

Under Personal Information Protection Act, the Society may collect, use and disclose information to administer Society's recruitment and employment obligations to its employees, contractors, volunteers and students. The collection, use or disclosure of personal information must be limited to the type and amount of information reasonably needed to fulfill the purpose of the collection, use or disclosure.

Only information which relates directly to and is directly necessary for the operation of the Society's programs and/or services is collected. In most circumstances, personal information is collected directly from the relevant individual or designated representative. Indirect collection occurs as permitted under the *Freedom of Information and Protection of Privacy Act* with the Vancouver Coastal Health Authority and with the consent of the individual or their authorized representative.

If personal information is to be used for a purpose not previously identified, the new purpose will be disclosed, and consent will be sought prior to such use occurring unless the use is authorized or required by law.

An individual may withdraw consent at any time, subject to legal or contractual restrictions, provided reasonable written notice of withdrawal is provided to the Society. Upon receipt of written notice, the Society will advise of likely consequence(s) of the withdrawal, which may include the Society's inability to provide certain services.

The Society does not sell information to third parties for any purpose.

Information and Privacy Protection

Access to personal information is administered using strict 'need to know' principles to ensure a minimum amount of personal information is accessed by those employees or contractors to perform their duties. Supervisors will regularly review an employee or contractor's access to electronic systems to ensure their access level remains appropriate.

Personal information is only used by authorized Society employees, contractors, volunteers and students to fulfill the purpose for which it was originally collected and to assess the services provided. Volunteers do not have access to resident health and financial information. The Society's Privacy Officer develops and maintains procedures to guide access to health records (**Appendix F)**.

Resident health records may only be released if there is written approval from the resident or authorized representative. Information released to authorized persons will not be made available to any other party without further authorization.

Personal Information and Privacy Act (PIPA) protects the privacy of individuals after death by regulating the collection, use and disclosure of personal information about a deceased individual that is in the custody or under the control of an organization. The Act also requires organizations to take reasonable security arrangements to protect that personal information.

The Society's Privacy Officer maintains guidelines for the release of information to third parties **(Appendix G).** The Society ensures personal information in its custody is accurate. If information is demonstrated to be inaccurate, the Society will amend the record and document the change.

To prevent unauthorized access, collection, use, disclosure and disposal of personal information, Society employees, contractors, volunteers and students make reasonable security arrangements to ensure the physical and technical security of all data. These steps should include:

- Removing documents with personal information from their desk/printers.
- Keeping information in locked cabinets.
- Cleaning whiteboards and removing flipcharts when they contain confidential information.
- Logging out of computers/laptops at the end of each work day.
- Shredding any materials that contain personal information – re-using and printing on papers containing personal information is prohibited.

To protect personal information, computers and laptops lock after 5 minutes of inactivity.

Wherever possible, users should not transmit sensitive information via e-mail without prior authorization.

Electronic records containing personal information must not be stored or accessed outside the Society's protected corporate network.

Employees and contractors may only work outside the Care Centre or Manor with personal information if they have their supervisor's approval and ensure electronic access is done so via secured remote connections – see "**Computer Network**" for more information.

Photography and Video

The Society may use photography and video captured at the Care Centre for various purposes – upon admission, residents or their designated representatives sign the Resident Consent form to authorize Three Links' use of photos and videos **(Appendix H)**.

The Society must ensure adequate notification is in place any time photographs and/or video recordings are collecting personal information of identifiable individuals. Whenever possible, the Society must ensure explicit and informed consent is received prior to imagery being collected. If an individual chooses not to be recorded they must not be refused access.

For larger public events, appropriate signage/notification must be prominently displayed to ensure all individuals are aware of photography prior *to* being included in the footage. Notification must include the purpose of collection, proposed use and contact information of the Society's Privacy Officer. The Privacy Officer develops and maintains a consent form that can be presented and completed whenever possible for the collection of photography (**Appendix I).**

If an individual does not wish to be photographed, they may contact the Society's Privacy Officer to ensure their image is not captured. Individuals may refuse to be recorded and their refusal must not hinder their right to participate in an event.

TECHNOLOGY

Computer Network

The Society respects the privacy of those who use the computer network and strives to apply the most current technology available to safeguard their privacy and the confidential data.

The Society maintains computer systems through which employees may be granted access privileges permitting remote access to the Society's records. The Society's Privacy Officer maintains the procedures that all staff and contractors with such privileges must comply with when accessing the Society's computer network (**Appendix J)**.

Access to systems is available at the discretion of the Executive team. Upon approval, the Information Technology contractor sets up remote access for the authorized users. The authorized users must use two-factor authentication (2FA), either Fortitoken or web-based 2FA to gain access to the Three Links network.

The Society's computer network may be used for reasonable personal use, provided it does not interfere with the User's work duties or create business risk to the Society. The following are

examples of unreasonable and unacceptable behavior when accessing the Society's computer network:

- Visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material.
- Using the computer to perpetrate any form of fraud, software, film or music piracy.
- Send offensive or harassing material to other users.
- Downloading commercial software or copyrighted materials belonging to third parties, unless permitted under a commercial agreement or other such licence.
- Hacking into unauthorized areas.
- Publishing defamatory and/or knowingly false material about Three Links, its team members or clients.
- Revealing confidential information in a personal online post, upload or transmission - including internal discussions.
- Introducing any form of malicious software into the corporate network.

The Society maintains cyber-security insurance and conducts regular tests of the computer network in collaboration with a dedicated and experienced Information Technology consultant.

Employees and contracted contractors must not divulge, share or compromise their own passwords and login details - including technical support staff.

The Society reserves the right to review any user's electronic files to ensure the employee's corporate network is being used in compliance with this guideline. This review must be authorized by the CEO and the user will be notified by the Society's Privacy Officer prior to the review.

Any software installation on Society's equipment (including mobile devices) requires manager's approval and must be installed by the Information Technology contractor.

Computer Equipment

The Society provides employees with the necessary computer equipment to perform their job functions.

Computer equipment and mobile devices provided to employees is property of the Society and must be returned upon the employee's departure from the organization. Any use of mobile storage devices, including phones, must be pre-approved by the Society's Privacy Officer.

All files containing personal information saved to a mobile storage device must be encrypted and secured through the use of a secure password.

Mobile storage devices are to be kept physically secure with limited access.

E-Mail

The Society provides employees, contractors and Board members with secure email accounts that must be used when conducting Society business. Any information transmitted through the Society email account is the property of the Society.

Whenever possible, transmitting personal information via email should be discouraged. When no option exists, documents containing personal information must be password protected prior to transmission.

The Society's Privacy Officer may restrict email access on mobile device provided by the organization.
Unacceptable use of the Society email may result in disciplinary action and access restrictions. The following behaviour is considered unacceptable when using the Society email:

- Set up or manage personal businesses.
- Accessing, distributing or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal.
- Accessing, distributing or storing images, text or materials that might be considered discriminatory, offensive, abusive, sexist or racist.
- Broadcasting personal views on social, political, religious or other non-business-related matters.
- Transmitting chain letters, unsolicited commercial or advertising material.

Wi-Fi Access

The Society facilitates Wi-Fi access throughout the Care Centre via 3 networks with various levels of security:

- **Three Links Visitors** - Free, public, non-encrypted access. Users must accept terms of use and reaffirm every hour. Available to residents and families, staff, contractors, volunteers, students and visitors for personal use.
- **Three Links Board** - Encrypted access for the exclusive use of Board members to conduct Society's business. No hourly reaffirmation of usage terms.
- **Three Links** - High level of encryption to facilitate access for management and select staff/ contractors to conduct Society's business.

Information Technology Contractor

While performing system maintenance, authorized IT consultants may inadvertently view or access data files or messages. When this occurs, they are required to keep the contents confidential, unless there are suspected violations of law or policy. These are reported to the CEO and the Society's Privacy Officer for further review.

Website

The Society maintains a website and social media accounts on a secure platform with an experienced contractor. The Society's Information Technology contractor runs regular tests on the website's security platform.

The Society's website may collect and store information from website visitors, including: internet protocol address and domain name used; type of browser and operating system; date and time of the visit; and web pages accessed. Information collected is used only for the purposes of administering the website, assessing system performance, improving services and website management.

Video and Digital Surveillance

To ensure the safety of residents, visitors, employees, contractors, volunteers, students and company equipment, the Society uses surveillance cameras, electronic key cards and punch clocks on its properties. At no times shall this technology be used to monitor employee productivity and performance.

The Society's Privacy Officer maintains a list of surveillance camera locations and ensures all entrances to the building have signs identifying the use of video surveillance. All cameras must be in plain view and only record activity on the Society's property. Some of the outdoor cameras may inadvertently capture the activity in public areas – the footage captured is only used to ensure the safety and security of the Society, its residents, visitors, employees, contractors, volunteers, students and company equipment.

In the event of a reported or observed incident, the recoded footage may be used to assist in the investigation of the incident. At no time with persons other than the Society's Privacy Officer or persons designated in writing by the Privacy Officer have access to this surveillance information.

Footage from surveillance cameras will be maintained for fifteen (15) days unless required for the purposes outlined in this policy. Footage used to investigate an incident is retained for at least one year after a final conclusion is reached concerning the incident. Footage not used will be erased so it is permanently unreadable.

Information from electronic key card data will be stored 90 days before being permanently deleted. Punch clock records containing employee information are stored for 7 years.

Video Conferencing

At times when face-to-face communication is difficult to achieve, Three Links uses video conferencing tools such as Facetime and Zoom. These applications are used for:

- Management, Board and other team meetings including those with external partners.
- Video calls between residents and their loved ones.

To ensure the privacy of all parties engaged in the video conferencing, Three Links representatives follow these guidelines:

- Only Three Links equipment (computers, laptops, tablets, etc.) connected to the Three Links' corporate systems to be utilized for all video conferencing, ensuring the devices are consistently patched. The use of personal devices is not permitted.
- Video conferencing applications used must be updated when prompted to remain secure.
- Resident calls should all be initiated by Three Links team members.
- Whenever possible, video connection should require a PIN or a password to join.
- Discussion of confidential information should be avoided when using video conferencing. Whenever possible, Three Links team members should switch to regular telephone lines to discuss confidential topics.

When using video software, Three Links representatives take the utmost care to protect personal information of our residents and their representatives, staff, contractors, volunteers and students.

HUMAN RESOURCES

Personal information pertaining to the Society's employees, contractors, volunteers and students will not be provided to persons from outside the organization without permission from the individual themselves (**Appendix G)**.

The Society may use employee information to manage the employment relationship and for other purposes authorized or required by law. The Society may use employee personal information to contact employees or their family in an emergency or for general hiring, employment and security purposes.

The Society may disclose information to third parties during these processes, including benefits providers, Canada Revenue Agency, WorkSafe BC, medical services agencies, Society lawyers and bookkeepers.

Only the Society's Privacy Officer may release personal information of employees, contractors, volunteers and students to law enforcement authorities upon receipt of appropriate court documents.

Employees have a right to access their personal information. Upon written request and authentication of identity, the Society's Privacy Officer will review the request with the applicant and provide employees with information under their custody and/or control within 30 days. If granted, request to access personnel file will be granted within 7 days. This disclosure may include information about ways information is being used and a description of the individuals or organizations to whom such information has been disclosed.

The Society may not be able to provide access where disclosure would reveal personal information about another individual, the information is subject of a current legal proceeding or where disclosure of the information would reveal confidential commercial information that could harm the Society's competitive position if disclosed. Where an access request is refused in whole or in part, the Society's Privacy Officer will notify the employee in writing with the reason for refusal and other steps available to the employee.

For more Information, contact Three Links Privacy Officer at privacyofficer@threelinks.com.

APPENDIX A – Summary of Consolidated Policies

AE0400 – Confidentiality of Information

AE0405 – Information Security - End of Day

AE0410 – Wireless Access

AE0415 – Network Access and Computer Use

AE0440 – Protection of Records When Working Away from the Workplace

AE0425 – Retention Storage and Destruction of Records

AE0525 – Privacy Policy; Resident Tenant

AE0530 – Privacy Breach Management

AE0900 – Facsimile Transmissions

AE1000 – Health Records Access To

AE1900 – Release of Resident Information

HRT 1000 – Confidentiality

HRT 1300 – Employee Privacy

APPENDIX B – Three Links Privacy Statement

OUR COMMITMENT TO PRIVACY

Three Links Care Society (Three Links) is subject to the *Personal Information Protection Act (PIPA)* and the *Freedom of Information and Protection of Privacy Act*. Three Links is committed to protecting the privacy of our residents and their representatives, staff, contractors, volunteers and students. It is Three Links' goal to not only meet our legislated requirements, but to exceed the requirements by implementing "best practices" with respect to the collection, use, disclosure and security of the personal information in our custody and control.

Three Links also requires our third-party service providers to demonstrate full compliance with our privacy obligations, principles and processes outlined in this policy.

Three Links only collects personal information as supplied by our our residents and their representatives, staff, contractors, volunteers and students in support of the programs and services we provide. Only that information which relates directly to, and is necessary for, the operation of our programs is collected. We do not collect personal information unlawfully or unfairly. In most circumstances, we only collect personal information directly from the relevant individual. Indirect collection occurs only in very limited and specific circumstances, or as required by law.

Collected personal information will only be used by authorized Three Links employees and contractors, to fulfill the purpose for which it was originally collected, for specific purposes if directed by the individual from whom the personal information is being collected, or for a use consistent with the original purpose.

Three Links does not sell, share or disclose your information to others for any type of mailing list.

Three Links, its employees, and contractors administer the highest security standards to ensure that the personal information in our custody and/or control is secured at all times. Physical and technical security of all data (including all data at rest or in transit) must meet the highest security standards.

If you have any questions regarding privacy protection at Three Links, please contact Three Links Privacy Officer at: 778-452-6510 or privacyofficer@threelinks.com.

The Three Links website may collect and store information from website visitors, including: internet protocol address and domain name used; type of browser and operating system; date and time of the visit; and web pages accessed. Information collected will be used only for the purposes of administering the website, assessing system performance, improving services and website management.

APPENDIX C – Three Links Whistleblower Policy

Policy

Three Links Care Society is committed to delivering high quality care in a professional and ethical manner and expects staff to conduct themselves with honesty, integrity and accountability.

Three Links shall behave ethically and professionally toward each other and toward residents, tenants and other members of the public.

Three Links shall put into place mechanisms to address concerns and issues when it is believed that possible wrongdoing has occurred.

Individuals will have a process to bring forward information about wrongdoing by Three Links staff in good faith and without fear of reprisal. Three Links takes seriously all reports of wrongdoing, and where appropriate, conducts objective and impartial investigations in a timely manner.

Three Links will not take any indirect or direct reprisal against: a person who, in good faith and based on reasonable belief, reports a wrongdoing, a person who acts as a witness in an investigation, or a person who carries out an investigation of wrongdoing.

To the fullest extent possible, Three Links treats as confidential, the identities of those involved in the reporting and investigation of a wrongdoing. All information collected during the course of investigation will remain confidential, except as necessary to conduct a fair investigation and to take corrective or remedial action, and except where disclosure is permitted or required by law.

This policy does not replace other established processes or reporting structures, nor does it replace or supersede reporting obligations mandated in legislation.

Definitions

Staff: all Board members, officers, employees, contractors, volunteers and students engaged by Three Links.

Wrongdoing: a wrongful act or misconduct by a Three Links staff. Wrongdoing may include:

a) Mistreatment of residents, staff or members of the public;
b) Actions that pose a danger to residents, public health or the environment;
c) Actions that are unlawful or not in compliance with any laws or regulations, theft, fraud, bribery or corruptions;
d) Unethical or unprofessional conduct;

e) Unauthorized use, misuse or waste of public funds or resources;
f) Non-compliance with procurement rules or other unfair trade practices;
g) Actions that are not in compliance with Three Links policies or procedures, internal financial controls or audit procedures; and
h) Continuing to act while in a real or perceived conflict of interest.

Roles and Responsibilities

Staff

Staff are encouraged to report any real or suspected wrongdoing through the appropriate management channels as described in Reporting Wrongdoing.

Management/Leadership Team (Directors and Supervisors)

Management are required to take reports of real or suspected wrongdoing seriously and respond appropriately within the scope of their responsibility.

Management should follow existing channels for handling issues, incidents or complaints and escalate reports of wrongdoing as necessary. Management may also report real or suspected wrongdoing as described in Reporting Wrongdoing.

Management will inform the reporter of a wrongdoing about actions taken in an appropriate and confidential manner befitting the nature of the report.

Management, in consultation with the Director of Human Resources, will take appropriate action should an investigation determine that a staff member under their supervision has committed an act of misconduct or wrongdoing.

Chief Executive Officer (CEO)

The CEO is responsible for the maintenance and operation of this policy, including:

a) Referring the report to an already established process;
b) Assessing the merits of a report and determining whether to investigate;
c) Conducting an investigation or assigning investigators;
d) At the conclusion of an investigation, ensuring findings and recommendations are made;
e) Communicating investigation results to parties concerned; and ensuring the reporter of wrongdoing is informed about actions taken in an appropriate and confidential manner befitting the nature of the report.

Chair of the Board

The Chair of the Board is responsible for the management of any reports of wrongdoing that concern Board Members, the CEO, or members of the Leadership Team. The Chair of the Board may engage external parties as required.

Recordkeeping

Records will be kept of any reports of wrongdoing and the investigation process. The CEO shall retain a copy of records relating to investigations and any resulting reports. Investigation outcomes shall be reported to the Board and to the Leadership Team.

Aggregate reports of investigation outcomes shall be forwarded semi-annually to the Three Links Care Society Board. These records shall include the following information:

- Number of complaints
- Nature of complaints
- The nature of the process of resolution (i.e. informal resolution, mutual resolution, investigation).

Aggregate reports shall not identify the individuals involved.

Procedures

Reporting Wrongdoing

Staff are encouraged to first discuss a real or suspected wrongdoing with their manager or another manager. Reports may be made verbally in person, or by telephone, or in writing by mail/email. Anyone who elects not to report a real or suspected wrongdoing directly to management may report the wrong doing to the Board.

Reports shall provide as much detail as possible, including the nature of the wrongdoing, the name of the person alleged to have committed the wrongdoing, and other pertinent information. The information shall be as precise as possible.

The report may also be delivered to:

Director of Operations and Housing
Three Links Care Society
2934 East 22nd Avenue
Vancouver, BC V5M 2Y4

Reports involving Board Members, the CEO or members of the Leadership Team shall be made in writing to the Board Chair and forwarded to:

Chair of the Board
Three Links Care Society
2934 East 22nd Avenue
Vancouver, BC V5M 2Y4

All correspondence shall be marked as “Private and Confidential”.

Investigating Allegations

Reports under this policy shall be investigated promptly. Within 45 days of receiving a report of wrongdoing, the CEO and/or Board Chair shall determine based on the evidence whether a formal investigation shall proceed.

The circumstances where a report may not proceed to a formal investigation are when:

a) The matter may be effectively resolved through an alternative, informal process with agreement of the parties involved;
b) The matter is more appropriately dealt with through another established process, such as the grievance procedure under a collective agreement or complaint under the Workplace Conduct Policy.
c) The matter is determined to be frivolous or vexatious (for a matter to be frivolous, vexations, or an abuse of process, the allegation must be such that no reasonable person would treat as bona fide);
d) The report fails to provide particulars of wrongdoing; or
e) The matter was not brought in good faith or on the basis of reasonable belief.

Matters relating to professional conduct shall be referred to the appropriate professional body for review. Based on the nature of the matter, and the professional body, the person making the report shall be updated where possible.

Exceptions

The policy is not intended to be the primary mechanism to address matters for which there are other established policies for the reporting and investigation of improper conduct or violations, including:

a) Labour agreement violations covered by collective agreements;
b) Reports on safety hazard and unsafe conditions made in accordance with the provisions of the Workers' Compensation Board's Occupational Health and Safety Regulations;
c) Misconduct related to behaviours identified in Three Links' Workplace Conduct Policy, which would be dealt with through the mechanisms identified in that policy;
d) Actions or incidents which constitute personal information that are handled through the Information Privacy Policy;
e) Resident safety or quality of care issues that are being handled through the Ministry of Health Patient Care Quality Review Board.

Related Policies

- Privacy Policy – Accountability
- HR Policy HRR1200 – Workplace Conduct
- HR Policy HRR0100 – Complaint Procedure
- Personal Information and Privacy Act (PIPA)
  http://www.bclaws.ca/civix/document/id/complete/statreg/03063_01
- Vancouver Coastal Health Whistleblower Policy
  http://shop.healthcarebc.ca/vch/VCHPolicies/D-00-11-30036.pdf
- Fraser Health Whistleblower Protection Policy
  https://www.fraserhealth.ca/-/media/Project/FraserHealth/FraserHealth/About-Us/Accountability/Policies/WhistleBlower-Policy-201807.pdf?la=en&hash=B05911C8799D8F2AABF2AFC7E4A7457A163C830A

APPENDIX D – Privacy Breach Protocol

A privacy breach is the unauthorized access, collection or disclosure of the personal information of individuals who live, work or volunteer at the Three Links Manor and Care Centre. Activity is unauthorized if it contravenes relevant privacy legislation or Society policy.

The Society's Privacy Officer will investigate all known or suspected incidences concerning a breach of privacy as outlined below:

STEP 1 – Report the breach or suspected breach

Any individual working on behalf of Three Links who becomes aware of a privacy breach or a suspected privacy breach must immediately inform their manager or designate. The Manager will notify the Privacy Officer. Where there is a potential conflict of interest, such reports may be made to the CEO.

The following information is required when reporting the breach:

- What happened and when?
- In which department?
- How and when was the incident discovered?
- What type of data was breached and which people are affected?
- Has any corrective action been taken?

The Society's Privacy Officer will verify the circumstances of the possible breach and inform the CEO. The incident will be documented in a privacy incident database maintained by the Privacy Officer.

Step 2 - Determine if a breach has occurred

The Society's Privacy Officer must determine if personal information is involved in the breach and if unauthorized access or disclosure took place. If they do not determine a breach took place, the Privacy Officer will inform the person reporting the breach about the outcome of the review.

Step 3 - If a breach has occurred

The Society's Privacy Officer will inform the person reporting the breach, director(s) of the affected department(s) and CEO. They will also inform the information technology consultant if breach has been caused by or relates to technology.

The Privacy Officer may assemble a committee of relevant managers, staff and contractors within 7 days to lead implementation of steps to correct the breach and keep it from happening again.

Step 4 – Contain the breach

The Society's Privacy Officer and department manager responsible will retrieve as much of the breached information as possible, destroy copies, ensure no additional copies have been made or retained, obtain the individual's contact information and ensure further breaches cannot occur through the same means.

Immediate steps may be taken to decrease the chances of the breach occurring. For example, if a letter has been mailed to a wrong address, contact the recipient, ask that it not be opened and have it returned to the Society.

Step 5 – Evaluate risks associated with the breach

The Society's Privacy Officer will consider the following factors to determine appropriate risk mitigation measures:

- What data elements have been breached? The more sensitive the data, the higher the risk. Health information and financial information that could be used for identity theft are examples of sensitive personal information.
- What possible use is there for personal information? Can the information be used for fraudulent or otherwise harmful purposes?
- What is the cause of the breach? Is there a risk of ongoing or further exposure of the information?
- What was the extent of the unauthorized collection, use of disclosure, (including the number of likely recipients) and the risk of further access, use or disclosure, including media or online?
- Is the information encrypted or otherwise not readily accessible?
- What steps have already been taken to minimize the harm? How many individuals are affected?
- Who was affected by the breach: residents and/or their designated representatives, staff, donors, volunteers, students?
- What harm to the individuals will result from the breach? What harm could result to Three Links?

In consultation with the CEO, the Privacy Officer shall notify the police if the breach involves or may involve any criminal activity.

If the risk is determined to significantly impact the reputation of the Society, the CEO will initiate a crisis communication plan. If the information technology security risk is high, the CEO may initiate an urgent recovery plan, in consultation with the Board and consultants.

STEP 6 – Notify affected individuals / institutions

The Society's Privacy Officer must notify every affected individual and advise them of personal information involved, potential harm that may occur, ways the affected individual can protect themselves and a Society contact that can respond to questions. The preferred method of notification is by phone or in person with a written follow-up.

Harms that can occur as a result of a privacy breach may include:

- Physical - Does the loss of information place an individual at risk of stalking or harassment?
- Hurt, humiliation - Could the loss of information damage an individual's reputation? This can occur with the loss of information such as medical records.
- Loss of business or employment opportunities - Could the loss of information result in damage to the reputation of an individual, affecting business or employment opportunities?
- Financial – May result in funds lost, disclosed financial information and/or identity theft.

Notification should occur within 2 – 4 days of the completed review. However, if law enforcement authorities have been contacted, it should be determined from those authorities whether notification should be delayed so as not to impede a criminal investigation.

There may be rare circumstances where it is determined that notification would cause further harm to the affected individual. These instances should be assessed thoroughly to weight the benefits of notification against potential negative impacts. Final determination of this will be made by the Society's Privacy Officer in consultation with the CEO.

Step 7 – Documentation, Investigation and Remediation

All details of a breach, suspected breach and containment strategy must be documented by the Society's Privacy Officer. Reports must include:

- nature and scope of breach
- events that led to the breach
- steps to manage the breach
- plans to notify individuals and other parties affected
- contact information for follow-ups and instructions given to the reporting party
- timetable for providing CEO with regular updates about the breach and its ongoing management
- recommendations for remedial action to prevent future breaches

A report on the investigation must be submitted to the CEO within 30 days of the breach being reported.

For more information, contact Three Links Privacy Officer at privacyofficer@threelinks.com.

PRIVACY BREACH CHECKLIST

Date of report:	
Date and time breach was initially discovered:	

A. Contact Information

Name of person who reported the breach / suspected breach:	
Job title and contact information:	
Name of manager (if applicable):	

B. Incident description

Describe the nature of the breach and its cause. How was it discovered and when? Where did it occur?

C. Containment and risk evaluation

Answer each of the following questions and then, based on those answers, complete the risk evaluation summary.

(1) Containment

Check all the factors that apply:

	The personal information has been recovered and all copies are now in our custody and control.
	We have confirmation that no copies have been made
	We have confirmation that the personal information has been destroyed
	We believe (but do not have confirmation) that the personal information has been destroyed
	The personal information was encrypted
	The personal information was not encrypted
	Evidence gathered so far suggests that the incident was likely a result of a systemic problem
	Evidence gathered so far suggests that the incident was likely an isolated incident
	The personal information has not been recovered but the following containment steps have been taken (check all that apply): - The immediate neighbourhood has been thoroughly searched - The IT department has been notified - All passwords and system user names have been changed
Describe any other containment strategies used:	

(2) Nature of Personal Information Involved

Check all the data elements involved (eg. name, date of birth, email, address, medical information, etc.):

	Name
	Email address
	Address
	Date of birth
	Financial Information
	Donor Information
	Medical Information
	Personal characteristics such has race, religion, sexual orientation
	Other (describe)

(3) Relationship

What is the relationship between the recipient of the information and the individuals affected by the breach?

	Stranger
	Friend
	Neighbour
	Ex-partner
	Co-worker
	Unknown
	Other (describe)

(4) Cause of the breach

Based on your initial investigation of the breach, what is your best initial evaluation of the cause of the breach?

	Accident or oversight
	Technical error
	Intentional theft or wrongdoing
	Unauthorized browsing
	Unknown
	Other (describe)

(5) Scope of the breach

How many people were affected by the breach?

	Very few (less than 10)
	Identified and limited group (between 10 and 50)
	Large number of individuals affected (more than 50)
	Numbers are not known

(6) Foreseeable harm

Identify the types of harm that may result from the breach. Some relate strictly to the affected individual; but harm may also be caused to Three Links and other individuals if notifications do not occur.

	Identity theft – most likely when the breach includes loss of SIN, credit card numbers, driver's licence numbers, debit card information, etc.
	Physical harm – when the information places any individual at risk of physical harm from stalking or harassment
	Hurt, humiliation, damage to reputation – associated with the loss of information such as medical health records, medical records, disciplinary records
	Loss of business or employment opportunities – usually as a result of damage to reputation to an individual
	Breach of contractual obligations – contractual provisions may require notification of 3rd parties in the case of data loss or privacy breach
	Future breaches due to technical failures – notification to the manufacturer may be necessary if a recall is warranted and/or to prevent a future breach by other users
	Other (specify) –

(7) Other factors

The nature of the relationship between Three Links and the affected individuals may be such that Three Links wishes to notify no matter what the other factors are because of the importance of preserving trust in the relationship. Consider the type of individuals that were affected by the breach.

	Resident
	Family member / Designated Representative
	Volunteer
	Employee
	Contractor
	Student
	Other (describe)

D. Risk Evaluation Summary

For each of the factors reviewed above, determine the risk rating. Refer to **Appendix C** as a guideline for assessment.

Risk Factor	**Risk Rating**		
	Low	**Medium**	**High**
1) Containment			
2) Nature of the personal information			
3) Relationship			
4) Cause of the breach			
5) Scope of the breach			
6) Foreseeable harm			
7) Other factors			
Overall Risk Rating			

Use the risk rating in **Appendix C** to help decide whether notification is necessary and design your prevention strategies. Foreseeable harm from the breach is usually a key factor in deciding whether or not to notify affected individuals.

In general, a medium or high risk rating will always result in notification of the affected individuals. A low risk rating may also result in notification depending on the unique circumstances of each case.

E. **Notification**

1) Should affected individuals be notified?

Once you have completed your overall risk rating, determine whether or not notification of affected individuals is required. If any of the following factors apply, notification should occur.

Consideration	Description	Factor applies
Legislation		
Risk of identity theft	Most likely when the breach includes loss of SIN, credit card number, debit card information, etc.	
Risk of physical harm	When the information places any individual at risk of physical harm from stalking or harassment	
Risk of hurt, humiliation, damage to reputation	Often associated with the loss of information such as mental health records, medical records or disciplinary records	
Loss of business or employment opportunities	Where the breach could affect the business reputation of an individual	
Explanation required	Three Links may wish to notify if the affected individuals include vulnerable individuals, or where individuals require information to fully understand the events, even when the risks have been assessed as low	
Reputation of Three Links	Where Three Links is concerned that the breach will undermine trust of stakeholders, it may decide to notify in order to ease concerns and to provide clear information regarding the risks and mitigation strategies undertaken, even when risks are assessed are low	

2) When and how to notify

When: Notification should occur as soon as possible following a breach. However, if law enforcement authorities were contacted, they should be consulted to determine whether notification should be delayed in order not to impede a criminal investigation.

How: The preferred method is direct – by phone, in writing or in person. Indirect notification via website information, posted notices or media should generally only occur where direct notification could cause further harm, is prohibitive in cost or contact information is lacking. Using multiple methods of notification in certain cases may be the most effective approach.

Considerations Favouring Direct Notification	**Check if Applicable**
The identities of individuals are known	
Current contact information for the affected individuals is available	
Individuals affected by the breach require detailed information in order to properly protect themselves from the harm arising from the breach	
Individuals affected by the breach may have difficulty understanding an indirect notification (due to mental capacity, age, language, etc.)	
Considerations Favouring Indirect Notification	
A very large number of individuals are affected by the breach, such that direct notification could be impractical	
Direct notification could compound the harm to the individuals resulting from the breach	

3) What to Include in Breach Notification Letters

The information included in the notice should help the individual to reduce or prevent the harm that could be caused by the breach. Include all of the information set out below:

Essential elements in breach notification letters	**Included**
Date of breach	
Description of breach	
Description of personal information affected	
Steps taken so far by Three Links to control or reduce harm	
Steps individuals can take to protect themselves	
Future steps planned by Three Links to prevent further privacy breaches	
Three Links contact information for further assistance	

4) Others to contact

Authority or organization	Reason for Contact	Applicable
Law Enforcement	If theft or crime is suspected	
Insurers	Where required in accordance with an	
Technology suppliers	If the breach was due to a technical falure	
Others (list)		

5) Confirm notifications completed

Key contact	Notified
Privacy Officer (Director of Operations and Housing)	
Your manager	
Chief Executive Officer	
Police	
Affected Individuals	
Legal Counsel	
Office of the Information and Privacy Commissioner of BC	
Others (list)	

PRIVACY RISK RATING GRID

Factor	Risk rating		
	Low	**Medium**	**High**
Nature of personal information	❒ Publicly available personal information not associated with any other information	❒ Personal information unique to the organization that is not medical or financial information	❒ Medical, psychological, counselling, or financial information or unique government identification number
Relationships	❒ Accidental disclosure to another professional who reported breach and confirmed destruction or return of the information	❒ Accidental disclosure to a stranger who reported the breach and confirmed destruction or return of the information	❒ Disclosure to an individual with some relationship to or knowledge of the affected individual(s), particularly disclosures to motivated family members, neighbours or co-workers ❒ Theft by stranger
Cause of breach	❒ Technical error that has been resolved	❒ Accidental loss or disclosure	❒ Intentional breach ❒ Cause unknown ❒ Technical error – not resolved
Scope	❒ Very few individuals affected	❒ Identified and limited group of affected individuals	❒ Large group of entire scope of group not identified (over 50)

Risk Rating Overview			
Factor	**Risk rating**		
	Low	**Medium**	**High**
Containment efforts	❒ Data was adequately encrypted ❒ Portable storage device was remotely wiped and there is evidence that the device was not accessed prior to wiping ❒ Hard copy files or device were recovered almost immediately and all files appear intact and/or unread	❒ Portable storage device was remotely wiped within hours of loss but there is no evidence to confirm that the device was not accessed prior to wiping ❒ Hard copy files or device were recovered but sufficient time passed between the loss and recovery that the data could have been accessed	❒ Data was not encrypted ❒ Data, files or device have not been recovered ❒ Data at risk of further disclosure particularly through mass media or online
Foreseeable harm from the breach	❒ No foreseeable harm from the breach	❒ Loss of business or employment opportunities ❒ Hurt, humiliation, damage to reputation or relationships ❒ Social/relational harm ❒ Loss of trust in Three Links ❒ Loss of Three Links assets ❒ Loss of Three Links contracts or business ❒ Financial exposure to Three Links including class action lawsuits	❒ Security risk (eg. physical safety) ❒ Identity theft or fraud risk ❒ Hurt, humiliation, damage to reputation may also be a high risk, depending on the circumstances ❒ Risk to public health or safety

APPENDIX E – Procedures: Document Retention, Storage and Destruction

Regardless of the format, records are managed and destroyed under the authority of the Society's Privacy Officer and in a manner consistent with retention periods prescribed by the BC *Personal Information Protection Act*, federal *Freedom of Information and Protection Act*, other provincial standards and criteria as established by the Society.

Resident records transferred to the Society from the Vancouver Coastal Health Authority remain the property of the Health Authority and must be retained indefinitely unless otherwise specified by them.

All other records are retained according to a Records Retention Schedule maintained by the Society's Privacy Officer. Retention periods are calculated from the end of the calendar year in which the record was created. The Society may retain records for an additional period if the Privacy Officer determines they have continued value.

All records that have exceeded the retention period in the Retention Schedule and any physical records no longer part of daily office use must be disposed of upon approval of the Privacy Officer.

Agreements with provincially recognized private records storage facilities are required to provide cost-effective and secure offsite storage, shredding and retrieval services. Storage facilities must be bonded, insured and meet appropriate international, national and provincial standards for records storage.

Once transferred to offsite storage, appropriate records are retained, destroyed or permanently housed for historical purposes according to their respective information schedules. An official Certificate of Destruction must be provided from a provincially recognized vendor and shall be retained by the Society's Privacy Officer indefinitely.

Records must either be placed in containers or boxes provided by the vendor. Records kept in storage must be properly labelled with the name of the generating department, the contents and the retention expiry date.

For more information, contact Three Links Privacy Officer at privacyofficer@threelinks.com.

THREE LINKS CARE SOCIETY

APPENDIX F - Procedure: Access to Health Records

Resident Chart Access

Residents have the right to access their own records which are in the possession of the Care Centre. Residents also have the right to designate one primary decision-maker and one financial contact, recognizing these can be the same person.

All requests for health record access shall be directed to the Society's Privacy Officer. The Privacy Officer may refuse access if the disclosure could threaten anyone's personal safety or mental/physical health or interfere with public safety. If access is refused, two supporting opinions are required from physicians familiar with the case.

Prior to granting access, the Society's Privacy Officer will review records to identify if:

- third party information may have to be severed from the records
- disclosure would reveal personal information about another individual
- personal information is protected by solicitor/client privilege
- information was collected for the purpose of an investigation
- disclosure reveals commercial information that could harm the competitive position of Three Links

A fee may be applied prior to the processing of a request for personal information. The Society's Privacy Officer will remain with the resident to explain the records and ensure security of the record. If the resident wishes, they can designate another individual to also be present. This designated individual must sign a privacy agreement stating they are acting in the best interests of the resident. The attending physician may also be notified. If the physician objects to the review of the records, the matter will be reviewed by the CEO for final decision.

Photocopying of resident information is not permitted unless written authorization is obtained from the resident or their legal guardian and the CEO.

Chart Access by or Disclosure to the Resident's Representative

Access may be granted with the written authorization of a person who can produce documented evidence he/she has the authority to act on the resident's behalf. This may include Court appointed trustee or guardian, Executor of an estate, primary contact or designated health decision-maker. These representatives must act on behalf of the resident.

In the case of a near relative, if it is determined that the person is not acting on behalf of the resident, then he/she is treated as a third party for the purposes of the request.

General Chart Access

Staff and contractors involved in the care of the resident are authorized to access health records. These include:

Physicians	Social Worker	Rehab Assistant	Dietitian	Dentist
Physiotherapist	Visiting Consultants	Recreation Workers	RN's, LPN's, RPN's	Dental Hygienist
Podiatrist	Care Aides	Spiritual Care	Unit Clerk	Music Therapist

Individuals requesting access to health records shall identify themselves to the Society's Privacy Officer or Director of Care, indicate why they need access to the record and provide verification of their identity and authorization to access the record. If the person making the request is not doing so as an employee, a request in writing to the Privacy Officer is required.

Consultants and inspectors may access health records as required by legislation or Health Authority. This may include assessors, licensing authority, consultants or surveyors as authorized by current policy. Students may have access only to the extent it is required for their training and under supervision of their Instructor/Preceptor.

The CEO may only access health records for the purpose of an investigation or in the event of potential legal action.

Chart Access by or Disclosure to Other Parties

The Society's Board may only access a resident's record in cases of litigation where instruction to legal counsel must be given or review of a Coroner's jury report. In all cases, access shall be by Board resolution and facilitated through the CEO. Other volunteers are not allowed chart access under any circumstances.

Resident information which has been transformed into statistics and does not identify a resident may be employed in management, planning and resident care evaluations.

Access requests for research projects must be submitted in writing to the Society's Privacy Officer. All resident information used in the project must be viewed on the premises.

For more information, contact Three Links Privacy Officer at privacyofficer@threelinks.com.

APPENDIX G: Release of Information to Third Parties

The Society's Privacy Officer shall obtain written authorization from staff, contractors, volunteers, students, residents or their designated representatives prior to release of any personal information.

The Privacy Officer may only release information to verified medical personnel without resident authorization if information is being utilized for a purpose consistent with that for which it was collected.

The Privacy Officer may only release information to authorized individuals or agencies acting in the resident's best interest. This authorization includes, but is not limited to:

Statutory Authority

Automobile Insurance Act	I.C.B.C.
Coroners Act	Coroner
Criminal Code	R.C.M.P.
Criminal Injuries Compensation Act	W.C.B.
Health Act	Medical Health Officer, B.C. Cancer Agency
Hospital Act	Hospital Care, MOH
Medical Practitioner's Act	College of Physicians & Surgeons
Medical Services Act	M.S.P.
Worker's Compensation Act	W.C.B.

Judicial Order

Court Order/Subpoena	Civil Action
Search Warrant	R.C.M.P./Local Police
Subpoena	Crown Counsel
Summons/Order	Coroner

No information is to be given to media, insurance agencies or lawyers without the written authorization of the resident or their authorized representative and approval by the CEO. Society employees shall refer all requests for information by the police to the CEO.

All individuals seeking information from the Society or updating information about a resident, employee or themselves, must be verified before any disclosure may occur. This verification must be limited to four (4) out of the following six (6) pieces of personal information:

Resident Name	Contact name	Billing Address
Resident Date of Birth	Contact phone number	Contact E-mail

If a Society representative is not satisfied with the verification responses provided, the individual will be invited to submit their request in writing to the Society's Privacy Officer.

THREE LINKS CARE SOCIETY

APPENDIX H - Resident Consent for Photography, Outings and Hairdressing

Photography (Consent to have photos taken for the purpose of:)	**YES**	**NO**
Identification, Security, Resident Records		
Medical Treatment (Treatment (i.e. wound care), Education, Research)		
Facility Only (Internal Facility Photo Albums, Activity Posters and Bulletin Boards)		
Public (Website, Newsletters, Brochures, TV, Newspaper and Videography)		
Outings		
Authorize Three Links Care Society Recreation Staff and Volunteers to escort residents on organized outdoor activities. **NOTE:** Residents will not be included in outings activities if acutely ill, physically unable to participate, or have socially inappropriate behaviour.		

Hairdressing
(MUST be authorized by Financial Representative)

Shampoo Only ☐ Once a week ☐ Once every 2 weeks ☐ Once a month ☐ Upon request	**Shampoo/Set** ☐ Once a week ☐ Once every 2 weeks ☐ Once a month ☐ Upon request	**Haircut** ☐ Once a month ☐ Upon request
Permanent ☐ Every 3 months ☐ Upon request	**Tint/Colour** ☐ Once a month ☐ Upon request	☐ No Service

Date:_____ Resident Name: _____

Resident (signature):_____

Designate (signature):_____ Relation:_____

Witness:_____ Position: _____

Original: Resident Chart
Copy to Three Links Care Society Privacy Officer
Copy to Recreation Department
Copy to Hair Dresser

THREE LINKS CARE SOCIETY

APPENDIX I - Consent Form: Collection of Photography

Personal Information Consent for the Collection Use and/or Disclosure of Photographs/Videos

The personal information requested on this form will be used to record your consent for the collection and use of photographs and/or videos.

Name of Youth: (if applicable) ***(please print)***			
Name of Adult: ***(please print)***			
Phone Number:		**Email Address:**	

*** Shaded area denotes fields to be completed by Three Links Care Society**

Event:	
Description of the Personal Information being collected used and/or disclosed:	Photographs(s) _____ Video Recordings _____ identifying the individual(s) named above appearing at or participating in the above noted public event.

COLLECTION OF PERSONAL INFORMATION:

The personal information indicated above will be collected for the purpose of:_____ in accordance with the *Personal Information Protection Act.*

USE AND DISCLOSURE OF PERSONAL INFORMATION:

The photographs will be used for: (please include any third party disclosures):

_____

The personal information is not shared with any other third parties (unless listed above) except as requested by you, and is securely stored at all times. Please note that these recordings may be published on the Three Links Care Society website, and as such, will be publicly available. Three Links Care Society takes every precaution to protect this personal information however, Three Links is not responsible for any further unauthorized use or disclosure of the personal information available on our website.

THREE LINKS CARE SOCIETY

For Adults:

_____ I consent to the Three Links Care Society's collection, use and/or disclosure of my personal information according to the terms outlined above.

_____ I do not consent to the Three Links Care Society's collection, use and/or disclosure of my personal information according to the terms outlined above.

_____ _____

Signature Date

.../2

For Youth: a parent or legal guardian must provide name and signature if the youth is under 18 years old. Please check applicable box: ☐ **Parent** ☐ **Legal Guardian**

Name of Youth: _____
(please print)

I, _____, am the parent or legal guardian of the youth named above and I
Parent or Legal Guardian name (please print)
hereby **consent** to the collection and use/disclosure of the youth's personal information as indicated above.

_____ _____

Parent or Legal Guardian Signature Date

I, _____, am the parent or legal guardian of the youth named above and I
Parent or Legal Guardian name (please print)
hereby **do not consent** to the collection and use/disclosure of the youth's personal information as indicated above.

_____ _____

Parent or Legal Guardian Signature Date

The BC *Personal Information Protection Act*: This Act applies to nonprofit societies, in British Columbia. The purpose of the Act is to protect personal privacy by preventing the unauthorized collection, use and/or disclosure of personal information. The Act defines personal information as "recorded information about an identifiable individual …" and defines a record as including "books, documents, maps, drawings, photographs …" and "any other thing on which information is recorded or stored…". If you wish to allow the Three Links Care Society to take and use photographs of you as specified above, your written consent is required pursuant to the Act.

THREE LINKS CARE SOCIETY

APPENDIX J – Guidelines: Computer Network Access and Use

Only users who have been permitted to use the corporate network and have been granted a password may use the computer system. Unauthorized use or attempts to read, copy, modify or delete e-mail messages of other users is prohibited.

Users must not share computer or email passwords to anyone under any circumstances. If passwords are forgotten, the user must advise the Society's Privacy Officer so it can be reset. Users are required to change their login passwords on a regular basis.

All users of the corporate network must sign and abide by a Confidentiality Agreement prepared by the Privacy Officer. User access privileges will be determined by their reporting Director and reviewed on a regular basis to ensure that only the information required for the user to perform their duties is accessible. Computers/laptops connected to the network lock after 5 minutes of inactivity. To unlock, users must enter their password to continue. Remote network users must ensure security measures are maintained.

Users of mobile storage devices or remote access hardware supplied by the Society are responsible for ensuring reasonable measures are taken to prevent loss or theft. Users must not remove or relocate equipment/software without approval from the Society's Privacy Officer.

Information technology consultants must respect the privacy and security of any information not intended for public dissemination that becomes known to them by any means, deliberate or accidental. These consultants must obtain permission from the user prior to any access of their corporate network.

To prevent cyberattacks, users are required to apply the following approaches:

- Do not open emails or download attachments from anyone you do not know.
- If you do receive an email from someone you know but it "does not seem right", delete without opening it.
- Do not reply to spam or forward chain emails.
- Do not click on links in emails unless you are sure of the identity of the sender.
- Do not share personal bank or credit card information by email.
- If email correspondence claims to come from your bank, phone your branch to verify.
- Restart your computer at the end of each work day to ensure the latest security updates are installed

The Society facilitates Wi-Fi access throughout the Care Centre via 3 networks with various levels of security:

- Three Links Visitors - Free, public, non-encrypted access. Users must accept terms of use and reaffirm every hour. Available to residents and families, staff, contractors, volunteers, students and visitors for personal use.
- Three Links Board - Encrypted access for the exclusive use of Board members to conduct Society's business. No hourly reaffirmation of usage terms.
- Three Links - High level of encryption to facilitate access for management and select staff/ contractors to conduct Society's business.

For more information, contact the Three Links Privacy Officer at privacyofficer@threelinks.com.

THREE LINKS CARE SOCIETY

APPENDIX K – Consent for Treatment

I the undersigned do hereby consent for _____ (Resident name) to receive the following treatments:

	Yes	No
Medical treatment by a physician(s)	☐	
Routine dental care as required	☐	☐
Other approved professional treatment	☐	☐
Diagnostic procedures/tests as required	☐	☐
Transfer to hospital if deemed necessary by qualified medical staff	☐	☐
Release of resident remains to the funeral home on behalf of the Substitute Health Care Decision Maker	☐	☐
I understand that the facility participates in educational training for students from recognized health care programs, and that there may be students who participate in resident care under the supervision of authorized personnel.	☐	☐

Signed: _____ _____
(Resident or Substitute Decision Maker*) (Relationship to resident, if not the resident)

Print name: _____ _____
(If not resident) (Date)

Witness: _____ _____
(Signature) (Print name of Witness)

* Possible Substitute Decision Makers for health care consent include:

- A Committee of the Person
- A Representative as appointed by a "Standard" Representation Agreement (no lawyer required, but restrictions as to the authority will apply)
- A Representative as appointed by an "Enhanced" Representation Agreement (certified by a lawyer)
- A "Temporary Substitute Decision Maker" (*Appointment of a Temporary Substitute Decision Maker* form must be completed OR a TSDM referral made to the office of the Public Guardian & Trustee)

The Society may collect personal information of its residents and designated representatives as authorized by law to:

- Manage and administer occupant residency at the Three Links Care Centre and Three Links Manor;
- Provide required services or services requested by the resident or their authorized representative - and to assess those services;
- Provide information to third party contractors and medical professionals involved in the resident's care and/or treatment.

PIPA protects the privacy of individuals after death by regulating the collection, use and disclosure of personal information about a deceased individual that is in the custody or under the control of an organization. The Act also requires organizations to take reasonable security arrangements to protect that personal information.

THREE LINKS CARE SOCIETY

APPENDIX L – Confidentiality Agreement (Employee)

Confidentiality Agreement*

I acknowledge that I have read and understood the Three Links Care Society ("Three Links") policies and procedures on privacy, confidentiality and security.

I understand that:

- all confidential and/or personal health information that I have access to or learn through my employment or affiliation with Three Links is confidential
- as a condition of my employment or affiliation with Three Links, I must comply with these policies and procedures, and
- my failure to comply may result in the termination of my employment or affiliation with Three Links and may also result in legal action being taken against me by Three Links and others.

I agree that I will not access, use or disclose any confidential and/or personal health information that I learn of or possess because of my affiliation with Three Links, unless it is necessary for me to do so to perform my job responsibilities. I also understand that under no circumstances may confidential and/or personal health information be communicated either within or outside of Three Links, except to other persons who are authorized by Three Links to receive such information.

I agree that I will not alter, destroy, copy or interfere with this information, except with authorization and in accordance with Three Links' policies and procedures.

I agree to keep any computer access codes (eg. passwords) confidential and secure. I will protect physical access devices (eg. keys and badges) and the confidentiality of any information being accessed.

I will not lend my access codes or devices to anyone, nor will I attempt to use those of others. I understand that access codes come with legal responsibilities and that I am accountable for all work done under these codes. If I have any reason to believe that my access codes or devices have been compromised or stolen, I will immediately contact my supervisor or the Three Links Privacy Officer.

_____	_____
Employee Name	Employee Signature
_____	_____
Department Manager/Network Administrator	Signature
_____	
Date	

* This agreement will be kept in the employee's personnel file for the duration of the individual's employment/affiliation with Three Links.

Under Personal Information Protection Act, the Society may collect, use and disclose information to administer Society's recruitment and employment obligations to its employees, contractors, volunteers and students. The collection, use or disclosure of personal information must be limited to the type and amount of information reasonably needed to fulfill the purpose of the collection, use or disclosure.

THREE LINKS CARE SOCIETY

APPENDIX M – Privacy Protection Schedule (Contractor)

Privacy Protection Schedule

This schedule forms part of the agreement between the Three Links Care Society (THREE LINKS) and [Name of the Contractor] (the "Contractor") respecting Contract # N/A (the "Agreement").

Definitions

1. In this Schedule,
   (a) "access" means disclosure by the provision of access;
   (b) "Acts" means the *Personal Information Protection Act* and the *Freedom of Information and Protection of Privacy Act* as applicable.
   (c) "contact information" means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual;
   (d) "personal information" means recorded information about an identifiable individual, other than contact information.

Purpose

2. The purpose of this Schedule is to:
   (a) Enable THREE LINKS to comply with the Acts with respect to personal information; and
   (b) Ensure that, as a service provider, the Contractor is aware of and complies with the Act and with respect to personal information.

Collection of personal information

3. Unless the Agreement otherwise specifies or THREE LINKS otherwise directs in writing, the Contractor may only collect or create personal information that is necessary for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.
4. Unless the Agreement otherwise specifies or THREE LINKS otherwise directs in writing, the Contractor must collect personal information directly from the individual the information is about.
5. Unless the Agreement otherwise specifies or THREE LINKS otherwise directs in writing, the Contractor must tell an individual from whom the Contractor collects personal information:
   (a) the purpose for collecting it;
   (b) the legal authority for collecting it; and,
   (c) the title, business address and business telephone number of the person designated by THREE LINKS to answer questions about the Contractor's collection of personal information.

Accuracy of personal information

6. The Contractor must make every reasonable effort to ensure the accuracy and completeness of any personal information to be used by the Contractor or THREE LINKS to make a decision that directly affects the individual the information is about.

Requests for access to personal information

7. If the Contractor receives a request for access to personal information from a person other than THREE LINKS, the Contractor must promptly advise the person to make the request to THREE LINKS unless the Agreement expressly requires the Contractor to provide such access and, if THREE LINKS has advised the Contractor of the name or title and contact information of an official of THREE LINKS to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

Correction of personal information

8. Within 5 business days of receiving a written direction from THREE LINKS to correct or annotate any personal information, the Contractor must annotate or correct the information in accordance with the direction.
9. When issuing a written direction under section 8, THREE LINKS must advise the Contractor of the date the correction request to which the direction relates was received by THREE LINKS in order that the Contractor may comply with section 10.
10. Within 5 business days of correcting or annotating any personal information under section 8, the Contractor must provide the corrected or annotated information to any party to whom, within one year prior to the date the correction request was made to THREE LINKS, the Contractor disclosed the information being corrected or annotated.

Protection of personal information

11. The Contractor must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal, including any expressly set out in the Agreement.

Storage and access to personal information

12. Unless THREE LINKS otherwise directs in writing, the Contractor must not store personal information outside Canada or permit access to personal information from outside Canada.

Retention of personal information

13. Unless the Agreement otherwise specifies, the Contractor must retain personal information until directed by THREE LINKS in writing to confidentially dispose of it or deliver it as specified in the direction.

Use of personal information

14. Unless THREE LINKS otherwise directs in writing, the Contractor may only use personal information if that use is for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement, and in accordance with section 13.

Disclosure of personal information

15. Unless THREE LINKS otherwise directs in writing, the contractor may only disclose personal information to any person other than THREE LINKS if the disclosure is for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement or as directed by THREE LINKS.
16. Unless the Agreement otherwise specifies or THREE LINKS otherwise directs in writing the Contractor must not disclose personal information outside Canada.

Inspection of personal information

17. In addition to any other rights of inspection THREE LINKS may have under the Agreement or under statute, THREE LINKS may, at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect any personal information in the possession of the Contractor or any of the Contractor's information management policies or practices relevant to its management of personal information or its compliance with the Schedule. The Contractor must permit, and provide reasonable assistance to, any such inspection.

Compliance with the Act and directions

18. The Contractor must in relation to personal information comply with:
    (a) the requirements of the applicable Act, including any applicable order of the Commissioner under the applicable Acts; and
    (b) any direction given by THREE LINKS under this Schedule.

19. The contractor acknowledges that it is familiar with the requirements of the Acts governing personal information that are applicable to it as a service provider to THREE LINKS.

Notice of non-compliance

20. If for any reason the Contractor does not comply, or anticipates that it will be unable to comply, with a provision in this Schedule in any respect, the Contractor must promptly notify THREE LINKS of the particulars of the non-compliance or anticipated non-compliance and what steps it proposes to take to address, or prevent recurrence of, the non-compliance or anticipated non-compliance.

THREE LINKS CARE SOCIETY

Termination of agreement

21. In addition to any other rights of termination which THREE LINKS may have under the Agreement or otherwise at law, THREE LINKS may terminate the Agreement by giving written notice of such termination to the Contractor, upon any failure of the Contractor to comply with this Schedule in a material respect.

Interpretation

22. In this Schedule, references to section by number are to sections of this Schedule unless otherwise specified in this Schedule.
23. Any reference to the "Contractor" in this Schedule includes any subcontractor or agent retained by the Contractor to perform obligations under the Agreement and the Contractor must ensure that any such subcontractors and agents comply with this Schedule.
24. The obligations of the Contractor in this Schedule will survive the termination of the Agreement.

I have read and understand the above Privacy Protection Schedule

_____ _____

Contractor's Name Date

Under Personal Information Protection Act, the Society may collect, use and disclose information to administer Society's recruitment and employment obligations to its employees, contractors, volunteers and students. The collection, use or disclosure of personal information must be limited to the type and amount of information reasonably needed to fulfill the purpose of the collection, use or disclosure.

THREE LINKS CARE SOCIETY

APPENDIX N – Volunteer Agreement

Volunteer Agreement

I _____, understand my rights and responsibilities as a Volunteer with Three Links Care Society.

I have read the Policies and Procedures outlined in the Three Links Volunteer Handbook and agree to follow them.

I understand that compliance with the Policies and Procedures is important to preserve the quality of services offered to our residents and critical to the safety and well-being of the residents and their designated representatives, staff, contractors, volunteers, students and general public.

Furthermore, I understand that any breach of the policies will be taken seriously, and could be cause for discipline, suspension, or dismissal. I agree to seek advice from my supervisor if I am ever in doubt about any policy or any aspect of my volunteer role.

Signed: _____ Date: _____

Confidentiality Agreement

I _____, understand that I may come into contact with confidential information during the course of my volunteer duties.

Confidential information includes, but is not limited to, medical, financial, and personal details about residents, family members/designated representatives, staff, students and other volunteers.

I agree not to share any confidential information with other volunteers or people outside Three Links Care Society. I understand that this agreement remains in effect even when I am no longer a volunteer at Three Links Care Society.

If I suspect any breach of privacy or confidentiality, I will report it to the Coordinator of Volunteers immediately.

I understand that a breach of this confidentiality agreement will be grounds for disciplinary action.

Signed: _____ Date: _____

Under Personal Information Protection Act, the Society may collect, use and disclose information to administer Society's recruitment and employment obligations to its employees, contractors, volunteers and students. The collection, use or disclosure of personal information must be limited to the type and amount of information reasonably needed to fulfill the purpose of the collection, use or disclosure.

THREE LINKS CARE SOCIETY

APPENDIX O – Board of Directors Code of Conduct, Confidentiality and Conflict of Interest Guidelines

1. INTRODUCTION

The fundamental relationship between each Director and Three Links must be one of trust; essential to trust is a commitment to honesty and integrity. Ethical conduct within this relationship imposes certain obligations.

2. COMPLIANCE WITH THE LAW

(a) In his/her relationship with Three Links, no Director shall commit or condone an unethical or illegal act or instruct another Director, employee, or supplier to do so.

(b) Directors are expected to be sufficiently familiar with any legislation that applies to their work, to recognize potential liabilities and to know when to seek legal advice. If in doubt, Directors are expected to ask for clarification.

(c) Falsifying the record of transactions is unacceptable.

(d) Three Links Directors must not only comply fully with the law, but must also avoid any situation which could be perceived as improper or indicate a casual attitude towards compliance.

3. CONFLICTS OF INTEREST

(a) In general, a conflict of interest exists for Directors who use their positions at Three Links to benefit themselves, friends or families.

(b) A Director must not use his or her position with Three Links to pursue or advance the Director's personal interests, the interests of a related person[1], Director's business associate, corporation, union or partnership, or the interests of a person to whom the Director owes an obligation.

(c) A Director must not directly or indirectly benefit from a transaction with Three Links over which a Director can influence decisions made by Three Links.

(d) A Director must not take personal advantage of an opportunity available to Three Links unless Three Links has clearly and irrevocably decided against pursuing the opportunity, and the opportunity is also available to the public.

(e) A Director must not use his or her position with Three Links to solicit clients for the Director's business, or a business operated by a close friend, family, business associate, corporation, union or partnership of the Director, or a person to whom the Director owes an obligation.

[1] related person means a spouse, child, parent or sibling of a director who resides with that director

(f) Every Director must avoid any situation in which there is, or may appear to be, potential conflict which could appear to interfere with the Director's judgment in making decisions in Three Links' best interest.

(g) There are several situations that could give rise to a conflict of interest. The most common are accepting gifts, favours or kickbacks from suppliers, close or family relationships with outside suppliers, passing confidential information to competitors or using privileged information inappropriately.

(h) Three Links requires full disclosure of all circumstances that could conceivably be construed as conflict of interest.

4. DISCLOSURE

a) Full discloser enables Directors to resolve unclear situations and gives an opportunity to dispose of conflicting interests before any difficulty can arise.

b) A Director must, immediately upon becoming aware of a potential conflict of interest situation, disclose the conflict in writing to the Board Chair. This requirement exists even if the Director does not become aware of the conflict until after a transaction is complete.

c) If a Director is in doubt whether a situation involves a conflict, the Director must immediately seek the advice of the Board Chair. It may also be appropriate to seek legal advice.

d) Unless a Director is otherwise directed, a Director must immediately take steps to resolve the conflict or remove the appearance that it exists.

e) If a Director is concerned that another Director is in a conflict of interest situation, the Director must immediately bring his or her concern to the other Directors attention and request that the conflict be declared. If the other Director refuses to declare the conflict, the Director must immediately bring his or her concerns to the attention of the Board Chair. If there is a concern with the Board Chair, the issue should be referred to the Governance Committee.

f) A Director is required to disclose the nature and extent of any conflict at the first meeting of the Board after which the facts leading to the conflict have come to that Directors attention. After disclosing the conflict to the Director: :

(i) must not take part in the discussion of the matter or vote on any questions in respect of the matter. However, the Director may be counted in the quorum present at the Board meeting.

(ii) must not attempt, in any way or at any time, to influence the discussion or the voting of the Board on any question relating to the matter giving rise to the conflict.

5. OUTSIDE BUSINESS INTERESTS

(a) Directors must declare possible conflicting outside business activities at the time of appointment. Notwithstanding any outside activities, Directors are required to act in the best interest of Three Links.

(b) No Director may hold a significant financial interest, either directly or through a relative or associate, or hold or accept a position as an officer or Director in an organization in a relationship with Three Links, where by virtue of his or her position in Three Links, the Director could in any way benefit the other organization by influencing the purchasing, selling or other decisions of Three Links, unless that interest has been fully disclosed in writing to Three Links.

(c) A "significant financial interest" in this context is any interest substantial enough that decisions of Three Links could result in a personal gain for the Director.

(d) These restrictions apply equally to interests in companies that may compete with Three Links in all of its areas of activity.

6. CONFIDENTIAL INFORMATION

(a) "Confidential information" includes proprietary, technical, business, financial, legal, resident, client or Director information which Three Links treats as confidential.

(b) Directors may not disclose confidential information to any outside person unless authorized.

(c) Similarly, Directors may never disclose or use confidential information gained by virtue of their association with Three Links for personal gain, or to benefit friends, relatives or associates.

(d) Directors are advised to seek guidance from the Board Chair of the CEO with respect to what is considered confidential.

7. INVESTMENT ACTIVITY

Directors may not, either directly or through relatives or associates, acquire or dispose of any interest, including publicly traded shares, in any company while having undisclosed confidential information obtained in the course of work at Three Links which could reasonably affect the value of such securities.

8. OUTSIDE EMPLOYMENT OR ASSOCIATION

A Director who accepts a position with any organization that could lead to a conflict of interest or situation prejudicial to Three Links interests, shall discuss the implications of accepting such a position with the Board Chair recognizing that acceptance of such a position may require the Director's resignation from the Three Links Board.

9. ENTERTAINMENT, GIFTS AND FAVOURS

(a) It is essential to efficient business practices that all those who associate with Three Links, as suppliers, contractors or Directors, have access to Three Links on equal terms.

(b) Directors and members of their immediate families should not accept entertainment, gifts or favours that create or appear to create a favoured position for doing business with Three Links. Any firm offering such inducement shall be asked to cease; a sustained business relationship will be conditional on compliance with this Code.

(c) Similarly, no Director may offer or solicit gifts or favours in order to secure preferential treatment for themselves or Three Links.

(d) Under no circumstances may Directors offer or receive cash, preferred loans, securities, or secret commissions in exchange for preferential treatment. Any Director experiencing or witnessing such an offer must report the incident to the Board Chair immediately.

(e) Gifts and entertainment may only be accepted or offered by a Director in the normal exchanges common to established business relationships. An exchange of such gifts shall create no sense of obligation.

(f) Inappropriate gifts received by a Director should be returned to the donor and may be accompanied by a copy of this Code.

(g) Full and immediate disclosure to the Board Chair of borderline cases will always be taken as good-faith compliance with this Code.

10. USE OF THE THREE LINKS' PROPERTY

(a) A Director requires Three Links' approval to use property owned by Three Links for personal purposes, or to purchase property from Three Links unless the purchase is made through the usual channels also available to the public.

(b) Even then, a Director must not purchase property owned by Three Links if that Director is involved in an official capacity in some aspect of the sale or purchase.

(c) Directors may be entrusted with the care, management and cost-effective use of Three Links property and should not make significant use of these resources for their own personal benefit or purposes. Clarification on this issue should be sought from the Board Chair.

(d) Directors should ensure all Three Links property which may be assigned to them is maintained in good condition and should be able to account for such property.

(e) Directors may not dispose of Three Links property except in accordance with the guidelines established by Three Links.

11. RESPONSIBILITY

(a) Three Links is determined to behave, and to be perceived, as an ethical organization.

(b) Each Director must adhere to the standards described in this Code of Conduct, and to the standards set out in applicable policies, guidelines or legislation.

(c) Integrity, honesty, and trust are essential elements of Three Links' success. Any Director who knows or suspects a breach of the Code of Conduct, Confidentiality and Conflict of Interest Guidelines has a responsibility to report it to the Board Chair.

(d) To demonstrate determination and commitment, Three Links requires each Director to review and sign the Code annually. The willingness and ability to sign the Code is a required of all Directors.

12. BREACH OF CODE

A Director found to have breached his/her duty by violating the Code of Conduct will be liable to censure or a recommendation for dismissal.

13. WHERE TO SEEK CLARIFICATION

The Board Chair or the Governance Committee Chair will provide guidance on any item in the Code of Conduct, Confidentiality and Conflict of Interest Guidelines. The Board Chair may at his/her discretion or at the request of a Director, seek the advice of outside legal counsel or other expert advisor.

I ACKNOWLEDGE that I have read and considered the Code of Conduct, Confidentiality and Conflict of Interest Guidelines for Directors of Three Links and agree to conduct myself in accordance with the Code of Conduct, Confidentiality and Conflict of Interest Guidelines for Directors.

_____
Signature

_____
Print Name

_____
Date

Under Personal Information Protection Act, the Society may collect, use and disclose information to administer Society's recruitment and employment obligations to its employees, contractors, volunteers and students. The collection, use or disclosure of personal information must be limited to the type and amount of information reasonably needed to fulfill the purpose of the collection, use or disclosure.

THREE LINKS CARE SOCIETY

APPENDIX P – Student Confidentiality Agreement

Three Links Care Society takes pride in providing opportunities for students to learn and practice their skills in their chosen fields in health care. Through these learning opportunities, access is provided to personal information about resident's health and medical information. We expect all students to maintain and respect the confidentiality of any information that they may be privy to during the length of their clinical practicum or learning experience at Three Links Care Centre. Students are required to wear their student identification badges at all times during placement. Access to the Nursing Stations will be denied to persons not wearing proper identification badges.

Confidentiality Expectation:

1. I will only access information of residents who have consented to having student participation in their care and treatment or in regard to formal research projects which have been reviewed and approved by Three Links Care Society. Access is granted only during periods of clinical placement for the duration of your practicum at Three Links Care Centre.
2. I will not divulge or discussed any resident information outside Three Links Care Centre. Breaches of confidentiality are subject to legal action. Any misuse of resident information will be grounds for Three Links Care Society seeking to deny further access to Three Links Care Centre for clinical training by the individual student.
3. Medical records are to be reviewed on the units and ensure that the records are kept secured at all times. Photocopying and photographing of any medical records is not permitted.
4. The use of cell phones or recording devices to take pictures/record voices of residents/staff/visitors/the building or record events on the premises is not permitted.
5. The use of removable devices such as USB stick is not permitted on the premises.
6. While Three Links Care Society is keen to support you in your training, it can only do so on the basis that confidentiality is respected. If you have any questions regarding the requirements of confidentiality, please ask your Practicum Instructor.

Agreement:

I understand the basis upon which access to resident information is granted and I agree to abide by the appointment to respect confidentiality.

Student Name: _____ Signature: _____

Date: _____

Department Manager: _____ Signature: _____

Date: _____

Under Personal Information Protection Act, the Society may collect, use and disclose information to administer Society's recruitment and employment obligations to its employees, contractors, volunteers and students. The collection, use or disclosure of personal information must be limited to the type and amount of information reasonably needed to fulfill the purpose of the collection, use or disclosure.