COMMUNITY LIVING DURHAM NORTH

PRIVACY

Policy No: A-7 (Administration)

Effective Date: September 15, 2011
Last Revision: September 29, 2015
Last Review:

Rationale:

To ensure compliance with legislation and to define Community Living Durham North's commitment to protecting the privacy of people receiving support, their families, employees, volunteers, members and donors.

Policy Statement:

Community Living Durham North is in compliance with the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) which has established rules governing the collection, use and disclosure of personal information in the context of commercial transactions. This legislation impacts CLDN chiefly in terms of the information it collects from employees for the purposes of payroll, direct deposit and the administration of their pension plans and group benefits. The information is also necessary in order to liaise with interested branches of government like the Family Responsibility Office.

CLDN is also in compliance with relevant provincial legislation: the *Personal Health Information Protection Act* (PHIPA) and the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA).

Finally, CLDN acknowledges that people have an expectation based in common law that any and all personal information shared with the agency will be received by it in the strictest confidence and will be so treated and maintained.

Senior staff will develop and communicate detailed procedures for the purpose of privacy protection.

Approved by: Colin Kemp
for the Board of Directors

Date: September 29, 2015

COMMUNITY LIVING DURHAM NORTH

PRIVACY

Procedure No: A-7-1	Effective Date: September 15, 2011
The Legal Landscape	Last Revision: September 29, 2015
	Last Review:

- Personal Information Protection and Electronic Documents Act (PIPEDA):

  - This is federal legislation and its impact upon CLDN is in the realm of commercial activity that is federally regulated. The act is largely concerned about the information that businesses collect from their customers, including things like purchasing patterns and credit history, which can potentially be sold to other businesses.

  - CLDN is a not-for-profit provider of social services; it does not have customers per se and it does not collect personal information from customers. Our customers are the people to whom we provide support, and their families, and our relationship with them is essentially non-commercial.

  - Neither is employee information covered by this act except when it is used in the federally-regulated commercial sector. For example, we collect information about employees' driver's licences, and about their driving record, because we need to share this information with the company that insures our vehicles. Therefore, we are accountable, under PIPEDA, for how this information is managed and protected.

  - The act defines personal information as anything factual or subjective that pertains to an identifiable person; e.g. age, gender, income, blood type, ethnicity, employee files (evaluations, disciplinary records), medical information, etc. The names of our employees, their titles, and their business addresses and business telephone numbers are not considered to be personal.

- Municipal Freedom of Information and Protection of Privacy Act (MFIPPA):

  - The Act requires that local government organizations protect the privacy of an individual's personal information existing in government records. It also gives individuals the right to request access to municipal government information, including records containing their own personal information.

  - The Region of Durham funds the supports we provide to a small number of people. It requires us to keep certain kinds of personal information on these people and it reserves the right to audit the information. It naturally requires agencies that it funds to comply with this legislation.

- Personal Health Information Protection Act (PHIPA):
  - This provincial law is designed to ensure that organizations that collect personal health information take steps to ensure that it is protected against theft, loss and unauthorized use and disclosure. CLDN collects health information from the people it supports, as it must do in order to provide quality care, and to a lesser degree, in more specialized circumstances, it also collects health information from its employees.

- Common Law expectations:

  - Even when legislation does not regulate how we can collect, manage or share information, people have an expectation in common law that their privacy will be protected.

  - An example of a common law application would be our use of audio-visual technology in certain program areas. PIPEDA does not apply because neither the programs nor our use of the technology are commercial in nature. PHIPA does not apply because the equipment does not collect health information. Nevertheless, supported people and employees whose images or voices are captured by the equipment have a right to expect that we will use them responsibly; see Policy B-10 *Electronic Surveillance*.

Procedure No: A-7-2	Effective Date: September 15, 2011
Fundamental Principles	Last Revision: September 15, 2013
	Last Review: September 29, 2015

All privacy legislation attempts to ensure essentially the same thing; i.e. that sensitive information is collected and managed in responsible ways. PIPEDA articulates ten (10) principles that must be observed, and CLDN organizes its privacy plan around them.

1. Be accountable:

   Because sensitive data is collected by multiple departments, from both supported people and employees, the C.E.O. is directly responsible for implementing our privacy plan and for ensuring that all employees are held accountable for protecting the confidentiality and security of the information which they control, or to which they have access.

   Where personal information is transferred to a third party (for example, the transfer of employees' banking information to a direct deposit payroll service), CLDN will seek to include a privacy protection clause in its contract with the third party to ensure that it is accountable and able to provide a suitable level of protection.

2. Identify why the information is required:

Before we collect information from a supported person or an employee, explain why it is needed and what we will do with it.

Toward this end, CLDN's privacy plan will include an inventory of our personal information holdings detailing the reason for collecting each different kind of information.

3. Obtain consent:

   Upon explaining in a meaningful way why a particular kind of information is needed, CLDN will obtain and document the person's consent. All completed consents will be filed as hard copies in the person's primary file and their presence documented in the AIMS database. When a new use is identified for information already in our possession, a new consent will be obtained. Express consent will be obtained whenever possible and in all cases when the information is considered sensitive. However, consent can be assumed (i.e. implied consent) when it can be reasonably inferred from the actions or expectations of the person. For example, if a parent wishes to be informed of her child's doings in our respite program, she is providing implied consent for us to enter her phone number into our database.

   Employees and supported people/families can decline to provide certain kinds of information, or they can withdraw their consent for us to use it. Employees are not obliged to share their cell phone numbers if they do not wish us to communicate with them in this way. And a supported person can decline to have his grandparents entered into our database. But other kinds of information are essential to maintain the relationship between CLDN and its employee, or between CLDN and the person receiving service. In either case, with respect to information that has already been collected, CLDN will distribute this policy and our privacy plan to both employees and supported people, who may then object to certain ongoing uses or disclosures.

4. Collect only what is reasonable, relevant and really necessary:

   CLDN's privacy plan will be audited on an annual basis by senior management and types of information that are no longer required will cease to be collected - and the existing stock destroyed, where appropriate.

   Reducing the information we collect reduces the risk of privacy violations through theft or inappropriate use; it also lowers the cost of collecting, storing, retaining and ultimately archiving data.

5. Limit the use, disclosure and retention of information:

   Personal information shall not be used or disclosed for purposes other than those for which it was originally collected, except with the consent of the individual, and except in circumstances where disclosure is required by law.

It is important to note that CLDN does not share, sell, trade or rent any personal information for financial gain.

See the release of information procedures that are detailed below.

6. Be accurate:

   CLDN will keep personal information as accurate, complete and up-to-date as necessary, taking into account its intended use and the interests of the employee, or the supported person, who provided it.

7. Use appropriate security safeguards:

   CLDN takes every reasonable precaution in order to protect personal information against loss or theft, and to safeguard it from unauthorized access, disclosure, copying, use or modification. Our technological tools such as passwords and security settings on electronic files are set out in Policy C-24 *Information and Communication Technology.* Physical measures designed to protect paper files include locked files, locked office space, and a building alarm system.

   However, given the potential for verbal breaches of confidentiality, and the fact that sensitive information on supported people is retained in widely dispersed residential settings, the discretion of employees and volunteers at every level is critical to safeguarding confidentiality. Employees and volunteers are made aware of this trust and both sign a *Pledge of Confidentiality* during their orientation. Failures to keep this trust will be subject to discipline.

   In the event CLDN discovers that personal information in its custody or under its control has been stolen, lost or accessed by an unauthorized person, it will notify the affected individual at the first reasonable opportunity.

8. Be open:

   This policy and our privacy plan that speaks to individual pieces of personal information will be shared with supported people and their families, and also with employees of the agency. They will also be publicly posted on the CLDN website.

9. Give people access to their information:

   People have a right to review personal information, about them, that is held by CLDN; in the case of unionized employees, access to Personnel files is stipulated in our collective agreements. They also have a right to know how we use the information, and with what other organizations, if any, the information is shared.

10. Provide recourse:

    CLDN will investigate all privacy violation complaints that it receives, and in light of substantiated complaints it will take appropriate measures to improve information handling practices. Such complaints should be addressed to the C.E.O. and forwarded to CLDN's main office at 60 Vanedward Drive, Port Perry. See Policy B-22 *Resolution of Concerns and Complaints* and also C-28 *Complaint Procedure - for Non-Unionized Staff.*

    Complainants will be advised that they also have recourse to the Office of the Privacy Commissioner of Canada and/or the Information and Privacy Commissioner of Ontario. A detailed guide to PIPEDA, published by the Office of the Privacy Commissioner of Canada, is at www.priv.gc.ca/information/guide_e.pdf.

Procedure No: A-7-3	Effective Date: September 15, 2011
The Release of Employee Information	Last Revision:
	Last Review: September 29, 2015

- Employee information is routinely shared with various government offices, and sometimes with other third party organizations, because it is a legal requirement that the information be released. Examples include:

  - Information required by WSIB. Employee consents are not required as per the Workers Safety and Insurance Act.

  - Records of Employment for separation purposes are also provided in accordance with statutory requirements. Employees may request this document for reasons unrelated to separation, in which case it will be processed in a timely manner. CLDN is also required to respond to follow-up inquiries from the Service Canada Centre (or E.I. Office).

  - The Family Responsibility Office can also make demands upon our payroll department without the consent of the concerned employee.

  - Union's have a right to basic contact information respecting members of their bargaining units, and generally rely on employers to collect, maintain and share this information.

- In other situations, information is released to third party organizations at the employee's express request. Such information will be made available in a manner that supports the employee's needs while also protecting his confidentiality.

  - Credit Checks – Employee requests should be submitted to the Human Resources Department. A letter will be addressed "to whom it may concern," and it will be

given to the employee who will be responsible for its direction. The letter will include only position, length of service, hourly or annual rate of pay, and hours worked.

- Reference Checks – All reference checks will be forwarded to Human Resources where they will be matched to a Release of Information Request form. CLDN will decline the request if the employee has not put this form on file. Where a release has been completed, the request will be referred to the Manager best able to assess the employee's performance. Where an informed and positive reference cannot be provided, the Manager, or HR, will provide the third party with the person's employment dates, title and work week.

  Staff not employed in a managerial capacity shall not respond to reference requests.

- Legal Requests – Where lawyers have been engaged to resolve private disputes, information is sometimes requested of the employer. CLDN will act upon these requests when the employee signs and submits an appropriate consent. CLDN reserves the right to charge the legal firm for its time in preparing the release.

- Personal Information Requests – From time to time, third parties request employee addresses or phone numbers. They may or may not identify themselves as friends, neighbours or creditors. Regardless, CLDN will not release such information without the prior consent of the employee.

- Personnel files contain personal information but the files are the property of Community Living Durham North. Given appropriate notice, employees have a right to review their file in the presence of management staff, and copies may be requested. In the case of unionized staff, our collective agreements contain specific language relating to file access.

Procedure No: A-7-4	Effective Date: September 15, 2011
Release of Supported People's Information	Last Revision: September 29, 2015
	Last Review:

- A physical file is the property of Community Living Durham North, but the personal information contained in them is the property of the person or family concerned. Thus, CLDN can make policy on confidentiality and file management, but the person or family maintains the right to privacy and to control the release of the information.

- Written authorization is required prior to the release of any information to an individual or agency outside of CLDN. Each instance in which written information is requested requires separate authorization; standing consents do not have sufficient validity. It is the responsibility of the Program Manager to obtain and file the hard copy consent in the person's primary file, to document its presence there in the AIMS database, and to then see to the timely release of the information.

- Consents also need to be occasion specific, so the forms exist in various formats (e.g. A-8 Media Consent and A-10 Consent to Disclose Information). Consents are also collected as part of the Support Plan Agreement.

- Authorization to release information is given by adults (over eighteen) and by the parent or legal guardian in the case of a child. Where an adult is unable to provide informed consent, CLDN will approach the family member who acts on his or her behalf.

- Written authorization is obtained via the Support Plan Agreement authorizing CLDN to share personal information among employees who are actively involved in the provision of support. However, given the degree of movement within the agency, the discretion of our employees is the chief factor in protecting the confidentiality of supported persons.

- The few people whose service is funded by the Region of Durham must sign a consent form to disclose personal information for the purpose of the annual file audit by Housing Services staff.

- Written authorization to release information is not required to release to:

    - MCSS; our funder's access to information is stipulated in our signed contract;
    - a public hospital where the person is being treated;
    - an attending physician or dentist;
    - a coroner or medical examiner;
    - a court of officer of the court.

Procedure No: A-7-5	Effective Date: September 15, 2011
Sealed Files	Last Revision:
	Last Review: September 29, 2015

- A person receiving service, or a family member, may request that a certain document be sealed. Also, a manager or director may decide that a particular Incident Report or assessment is sufficiently sensitive that it ought to be sealed. To seal a document is to seal it in a manila envelope inscribed: "This document can only be accessed with the permission of a director."

- The sealed document will be placed in the supported person's Primary Files. Primary Files are for key information and are housed at the main office and not archived until after death or discharge. A third party assessment pre-dating admission to CLDN would be sub-filed under *Admission and History*. A sensitive Incident Report prepared by CLDN staff would be sub-filed under *Assessments and Communication.*

- From time to time, an employee's departure is the subject of negotiation between the employer and the person's bargaining agent. And, sometimes, in these circumstances, the employee's Personnel file becomes sealed. The entire file is then sealed shut with a similar note indicating that it can only be re-opened by a director.

- When it becomes necessary to re-open any file (pertaining to a supported person or a former employee) the director will add to it a note documenting the reason for the re-opening. The file will then be re-sealed.

Procedure No: A-7-6	Effective Date: September 15, 2013
Research	Last Revision:
	Last Review: September 29, 2015

- In assessing the merits of a proposed research project that hopes to improve our understanding of intellectual disabilities, or promote best practice within the DS sector, CLDN will apply the fundamental principles that underlie Canadian privacy legislation and this policy.

  - We will be accountable, and no research project, whether conducted externally by a third party or internally by CLDN staff, will be permitted without the express approval of the C.E.O. or designate.

  - We will ask the necessary questions about why the research is relevant and what is to be done with the information collected or with the analysis of the data.

  - No research will proceed without the consent of the supported person; where he or she withholds consent, the research, if it occurs, must not include him or her. The purpose of the research will be explained to supported people in plain language formats, if appropriate, or it will be conveyed to the family member who has been asked to consent. Where no family member is available, the Office of the Public Guardian & Trustee will be asked to provide consent. No retribution or repercussion of any kind will be experienced by supported people who decline to participate in a research project.

  - In principle, CLDN supports research that will likely improve our understanding of intellectual disabilities, or promote best practices. However, people will not be asked to participate in research unless they can expect to receive at least an indirect benefit from having done so. And, it is understood that consent might be withheld if there is no direct and tangible benefit. The PG&T will typically decline to consent in the absence of a direct and tangible benefit.

  - With a view to limiting the use, disclosure and retention of information, CLDN will ascertain the credentials of the researcher; investigate the design of the research project, the specific activities in which the researcher will engage, and the use to which he intends to put his finished product. Substantial assurances are in place if an academic or graduate student has had their project vetted and approved by a university's ethics review board.

- Likewise, looking at questions of accuracy or research quality, and ensuring that appropriate security safeguards are implemented are functions of ascertaining the credentials and reliability of the researcher, and of investigating his research design and tools. CLDN will make these inquiries. It will also share with the researcher a copy of this policy and verify that his/her research will not violate any part of it. Further, CLDN will reserve the right to stipulate that the research methodology or, more likely, the researcher's schedule of activities, be adjusted in order better comply with this policy, better respect the needs and rights of supported people, or in order to accommodate logistical issues like the availability of staff.

- CLDN will be open and forthright in explaining to supported people and staff the purpose of the research and the reasons for our participation.

- CLDN will stipulate that it receive a copy of the paper or report that is the end product of the research and it will in turn provide access to our own stakeholders.

- Questions of definition may arise from time to time. For example, do we engage in research when we organize a focus group or issue a satisfaction survey? Probably not when these activities are conducted internally; but we will nevertheless respect the privacy of the people we support. People who complete a satisfaction survey have provided their implied consent. If they withhold their name from the survey their anonymity is protected. If they provide their name, it will be viewed by certain managerial and admin staff, but their views will not be made public in any way. Only aggregate data is shared within the agency and amongst stakeholders. If an entry in the "comments" section of as survey is noteworthy and merits being made public, that would only occur after we had obtained a subsequent specific consent.

- This procedure on research is written with the rights of supported people and their families in mind, but CLDN is no less committed to protecting the privacy of its employees. Where the opinions or attitudes of staff are of interest to researchers, CLDN will inquire into the credentials of the researcher, design methodology and expected outcomes of the project. But it will not attempt to measure the benefits, direct or indirect, that may accrue to participating staff. It will simply notify staff of the researcher's interest and permit them to make contact with the researcher, perhaps by clicking on a Survey Monkey link, if they so choose.

- However, some information collected by CLDN is essential to maintaining the employer-employee relationship. And some of it, like wage rates attached to job classifications, is not personal information at all, unless identifying information is also provided. Other kinds of information, like attendance statistics, are derived from personal information but are typically expressed in aggregate and completely anonymous

form. In certain circumstances, CLDN may decide to share this kind of anonymous, aggregate information with experienced and competent researchers, and it may do so without obtaining consent.

Approved by: Glenn Taylor
CEO

Date: September 29, 2015