Purpose

Community Living Grimsby, Lincoln, and West Lincoln (the Agency) is committed to protecting the privacy and confidentiality of staff, students, volunteers, and people supported. The Agency follows all required legislation and will ensure that any person whose position requires access to personal or sensitive information understands their responsibilities under this policy and applicable legislation.

Procedure

The Agency is committed to maintaining confidentiality and protecting the privacy of the personal information it collects, uses, or discloses on behalf of the people supported, staff, volunteers, students, or others associated with the Agency.

The Agency will comply with all relevant legislation including the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, and the *Personal Health Information Protection Act, 2004*, SO 2004, c 3, Schedule A.

All staff, volunteers, and students will protect and respect the privacy of the people and families that the Agency serves, other staff, volunteers, students, and the Agency itself.

In the event that there is a breach of confidentiality, the Agency will take all necessary action to mitigate any damage caused by the breach, and will report to the applicable authorities, as required.

All parties within the scope of this policy will receive training in matters of confidentiality and privacy during the Agency orientation process.

Authority to access and make use of personal or confidential information is associated with and restricted by the job duties of each position. Everyone to whom this policy applies is accountable for ensuring that personal or confidential information is only used as required to perform their current duties, and that such information is not disclosed to anyone who does not have a legitimate need to possess such information.

The management of each team/work area may establish and enforce practices to guide the appropriate use and protection of personal and confidential information.

Anyone who is required to remove personal or confidential information from the usual place of storage is accountable for protecting such information until it is safely returned to the usual place of storage.

Privacy Principles

1. **Be accountable:**
    - The Executive Director and the People and Culture Department are responsible for ensuring that all staff, volunteers, and students are held accountable for protecting the confidentiality and security of the information which they control, or to which they have access.
2. **Identify why the information is required:**
    - Before we collect personal information, the Agency will identify the purpose for the collection.
3. **Obtain consent:**

- Unless otherwise inappropriate, the knowledge and consent of the affected individual is required for the collection, use, or disclosure of their personal information.
- All completed consents will be filed within the applicable personnel files.
- When a new purpose is identified for information already in the Agency's possession, a new consent will be solicited unless it is otherwise inappropriate to do so.
- The Agency will endeavour to secure individuals' express consent where the Agency seeks to collect, use, or disclose sensitive information. Implied consent may be solicited in appropriate circumstances.
- An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The Agency will inform the individual of the implications of such withdrawal.

4. **Collect only what is necessary:**
    - The collection of personal information shall be limited to that which is necessary for the purposes identified by the Agency. Information shall be collected by fair and lawful means.
    - Reducing the information collected reduces the risk of privacy violations through theft or inappropriate use, and lowers the cost of collecting, storing, retaining, archiving, and destroying data.
5. **Limit the use, disclosure and retention of information:**
    - Subject to legal requirements, 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.
6. **Be accurate:**
    - The Agency will endeavour to keep personal information as accurate, complete and up-to-date as necessary for the purposes for which it is to be used.
7. **Use appropriate security safeguards:**
    - The Agency will protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. The nature and extent of safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage.
    - In the event that the Agency becomes aware of the loss of, unauthorized access to, or unauthorized disclosure of personal information resulting from a breach of the Agency's security safeguards, the Agency will notify the affected individual if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual.
8. **Be open:**
    - The Agency will make readily available to individuals specific information about its policies and practices relating to the management of personal information.
9. **Give people access to their information**:
    - Upon request, an individual shall be informed of the existence, use, and disclosure of their personal information, and shall be given access to that information. An individual

shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. Provide recourse:

- The Agency will investigate all privacy violation complaints that it receives, and will take appropriate measures to improve information handling practices as appropriate.
- Complaints should be documented on a Complaint and Feedback form and forwarded to the Executive Director and/or People and Culture Department.
- 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, as applicable.

Sealed Files

People supported, or their authorized representative, may request that a certain document be sealed. Supervisors or directors may decide that a document is sufficiently sensitive that it ought to be sealed. Physical documents that are sealed will be placed in a manila envelope inscribed: "This document can only be accessed with the permission of a director." Electronic documents will be sealed in an appropriate manner depending upon the relevant software.

When it becomes necessary to re-open any sealed file, the appropriate director will add a note documenting the reason for the re-opening. The file will then be re-sealed.

Responsibilities

It is the responsibility of all staff, students, volunteers, and other persons working on behalf of the Agency, whose positions provide access directly or indirectly to personal or confidential information, to ensure that such information is not inadvertently disclosed.

Management is responsible for ensuring that:

- Appropriate consents are obtained for the collection, use, and disclosure of personal information and third-party requests;
- Policies and procedures regarding collection, use, and disclosure of personal information are consistently adhered to;
- Systems and procedures are in place to ensure that records are kept private;
- Requests from persons for access to their files are responded to;
- Information is retained or destroyed as required;
- Complaints or breaches of policy are investigated; and
- Staff return any personal or confidential information in their possession upon request, when no longer required, or immediately upon termination of employment.

Staff, students, and volunteers are responsible for:

- Understanding and following policies and procedures regarding personal and confidential information;
- Ensuring that confidential information is not overheard or observed by people supported in the vicinity of work areas;
- Immediately reporting any breaches of confidentiality to their Supervisor;
- Keeping private passwords and access to personal or confidential information; and
- Returning to management any personal or confidential information in their possession upon request, when no longer required, or immediately upon termination of employment.