Sarnia Lambton Workforce Development Board	
DEPARTMENT: All Departments	**POLICY**
POLICY: Customer Privacy Policy	
ADOPTION DATE: March 3, 2020	**REVIEW DATE: March 3, 2020**

Purpose

To ensure all the Sarnia Lambton Workforce Development Board (SLWDB) programs and services are in compliance with privacy legislation set out in Personal Information Protection and Electronic Documents Act (PIPEDA) as well as through the Information and Privacy Commissioner of Ontario (IPCO).

SLWDB is committed to respecting the privacy of individuals and businesses—whether they are responding to one of our surveys, providing personal information, taking part in an event or using our website.

This policy applies to all goods and services that are delivered by the Sarnia Lambton Workforce Development Board, by any means including in person, by telephone, electronically, by mail, visually, orally or by written means.

The policy applies to all Employees, volunteers, Board Members and third parties who deal with the public on behalf of the Sarnia Lambton Workforce Development Board.

Responsibilities

The Chief Privacy Officer (CPO) is the Executive Director. The CPO's role is to ensure that SLWDB's policies and practices are in line with current Government of Canada privacy legislation, including PIPEDA, as well Ontario Privacy legislation, as outlined by the IPCO.

The CPO will respond to all internal and external privacy questions on behalf of the organization and will respond to any requests, corrections and complaints, including explaining the purposes for collection, use and disclosure of personal information and for filing complaints.

The CPO must track privacy incidents and breaches and work to prevent similar incidents from arising in the future. They will inform all employees and volunteers of new privacy issues raised by technological changes, internal reviews, public complaints and court decisions.

Definition

Personal information includes but is not limited to the following:

1. Any information beyond the name, title, business address, business e-mail and business phone number(s) of an individual.
2. Sensitive personal data such as financial or medical information, or personal identifiers such as the Social Insurance Number;
3. Any information that can result in identity theft or some other related fraud; or
4. Any information that can otherwise cause harm or embarrassment detrimental to an individual's career, reputation, financial position, safety, health or well-being.

Collection and Retention of Personal Information

1. Employees and volunteers are required to obtain consent before collecting personal information. Request to withdraw personal information can occur at any time.
2. The purpose for collection of personal information will be identified at the beginning of any project or overture of participation.
    a. Email addresses that have been collected in order to share electronic mailings will be retained until such time as an individual chooses to unsubscribe.
    b. Surveys will clearly state the purpose for the collection of personal information if requested.
    c. If personal information is gathered and combined from more than one source, it will NOT be used for anything other than the purpose consent was received for.
    d. Personal information will be destroyed after the completion of a project.
3. When no longer required for the purpose identified, personal information will be destroyed.
4. Personal information will be held in locked cabinets and/or in electronic files that are protected by physical keys and/or electronic passwords.
5. No personal information will be disclosed unless requested under legal proceedings. SLWDB will comply with all requests from relevant government agencies and the justice system.

Requests for Personal Information

1. Personal information can be requested at any time by contacting the CPO. Requests will be responded to within thirty (30) days.
2. Personal information will be provided to an individual at no cost.

Complaints

1. Complaints must be made to the CPO in writing or through suitable accessible equivalent.
2. Complaints will be dealt with within fifteen (15) days of receipt.
3. All complaints will be investigated by the CPO. When complaints are found to be justified, corrective measures will be taken, policies amended and employees retrained.

4. Complaints that are not successfully resolved can be followed up with the IPCO as well as the Office of the Privacy Commissioner of Canada.

Breach Protocol

A privacy breach is the loss of, unauthorized access to, or disclosure of, personal information. This can occur as a result of the theft or loss of information or data storage equipment, or the improper or unauthorized collection, use, disclosure, access, storage or disposal of information, including misdirected correspondence.

When SLWDB discovers or is made aware of a breach, we will take the following actions immediately:

1. Assessment and containment
    a. Describing the circumstances that gave rise to the privacy breach;
    b. Taking inventory of the personal information that was or may have been compromised;
    c. Identifying the parties whose personal information has been wrongfully disclosed or accessed, stolen or lost, or if this is not possible, identifying the groups of individuals likely to have been affected;
    d. Identifying any other relevant information (e.g., similar or related incidents);
    e. Removing, moving or segregating exposed information or files to prevent further wrongful access;
    f. Shutting down the web site, application or device temporarily to permit a complete assessment of the breach and resolve vulnerabilities;
    g. Attempting to retrieve any documents or copies of documents that were wrongfully disclosed or taken by an unauthorized person.
2. Notification to affected individuals
    a. SLWDB will notify all affected individuals as soon as possible following the breach to allow individuals to take actions to protect themselves against, or mitigate the damage from, identity theft or other possible harm.
    b. Care will be exercised in the notification process to not unduly alarm individuals, especially where SLWDB cannot confirm that certain individuals have been affected by the breach.
    c. Preference will be given to notifying affected individuals by telephone or in person.
    d. In the event that the individuals cannot be located or the number of individuals is so large that the task would become too onerous, SLWDB will post a conspicuous notice on our website and share this information through our monthly newsletter.
    e. A general description of the incident, including date and time;
    f. The source of the breach (an institution, a contracted party, or a party to a sharing agreement);
    g. A list of the personal information that has been or may have been compromised;
    h. Notification will include:
        i. A general description of the incident, including date and time;

ii. The source of the breach;
iii. A list of the personal information that has been or may have been compromised;
iv. A description of the measures taken or to be taken to retrieve the personal information, contain the breach and prevent reoccurrence;
v. Advice to the individual to mitigate risks of identity theft or to deal with compromised personal information
vi. The name and contact information of the CPO with whom individuals can discuss the matter further or obtain assistance;
vii. A reference to the effect that the IPCO has been notified of the nature of the breach and that the individual has a right of complaint to that office, when applicable;
viii. A reference to the effect that the Ministry of Labour, Training and Skills Development has been notified of the nature of the breach; and
ix. That SLWDB will continue to inform affected individuals of developments as the matter is further investigated and outstanding issues are resolved.

3. Notification to the IPCO
4. Notification to the Ministry of Labour, Training and Skills Development
5. Notification to the SLWDB Board Executive
6. Mitigation and prevention
    a. SLWDB will ensure that a plan is developed to mitigate the risks identified during the investigation and that the plan is implemented; and
    b. Inform the IPCO, the Ministry of Labour, Training and Skills Development and affected parties of any risk mitigation plan to be implemented.
7. Sharing of lessons learned
    a. Staff and volunteers will be trained on any new protocols that are developed.

Additional Contact Information

Information and Privacy Commissioner of Ontario
2 Bloor Street East,
Suite 1400
Toronto, ON
M4W 1A8
1-800-387-0073
https://www.ipc.on.ca/