Privacy Policy

Integration Action for Inclusion in Education and Community (Ontario), the “Corporation”

Privacy of Personal Information Policy Approved by the Board of Directors: December 10, 2020

This policy revokes the prior policy approved by the Board on December 11, 2004

The Corporation collects personal and sensitive information on members, donors, supporters and volunteers. The Corporation must comply with the Federal *Privacy Information Protection and Electronic Documents Act* (PIPEDA), which applies to the standards for personal information with respect to commercial activity.

The Corporation must also comply with the *Corporations Act* and other regulations that set the standards for the collection, use, disclosure and safeguarding of privacy of personal information and the individual right of access of their own information as it applies to members.

This policy meets the requirements of the *Corporations Act* and the *Privacy Information Protection and Electronic Documents Act*.

The collection, storage and use of personal information should be treated in a manner that is respectful of the individual and complies with all legislative requirements.

Privacy Officer

The Corporation has appointed Paula Boutis as its Privacy Officer. She will be responsible for the organization’s compliance with all privacy legislation.

The Privacy Officer’s duties are to:

1. review the Corporation’s policies and practices with regard to personal information;
2. implement the necessary changes to guarantee that the collection and retrieval of personal information follow the Corporation’s policy;
3. inform the directors, members, any employees, any contracted agents (that is, companies or contractors under contract to perform specific duties for the Corporation), volunteers and the public on how the Corporation treats personal information; and
4. receive and handle complaints.

Definition of Personal Information

For the application of this policy, personal information means:

1. The personal address, telephone number or email address of the individual;
2. Any identifying number assigned to an individual which can lead to their identification (e.g. Social Insurance Number);
3. Information about an individual's financial affairs, credit history and bank account and credit card information;
4. Information about membership dues or donations payment history;
5. Information relating to the race, national or ethnic origin, citizenship status, colour, religion, age, sex, sexual orientation, marital or family status of the individual;
6. Information relating to employment, education, disability, medical, psychiatric or psychological history:
7. Criminal records;
8. Correspondence sent to the Corporation that is of a private or confidential nature, and any replies from the Corporation that would reveal contents of the original correspondence;
9. The individual's name if it appears with other confidential information, e.g. financial information;
10. Employee information including résumés, salary and benefits, disciplinary action, bank account information, performance or disciplinary information.

Personal information does NOT include the name, position and business phone number of employees or contracted agents.

Personal information does NOT include statistical data, which is summarized in such a way as to not identify any individuals.

Business contact information and certain publicly available information such as name, address and telephone number (as published in telephone directories) are not considered personal information.

Collection of Information

Personal information will be collected and used only for the following purposes:

1. To solicit or approve membership;
2. To solicit or accept donations;
3. To facilitate registration in programs and workshops offered by the Corporation;
4. where consent is provided, personal information collected further to the Corporation's research initiatives;
5. To retain relevant information on board members, members or donors for government purposes;

Employees, contractors or other agents of the Corporation, including volunteers, must not seek out personal information unless it is relevant to the work of the Corporation as outlined in this policy.

All documents used for collection of personal information shall state:

1. the purpose or purposes of the collection;
2. the reasons for collection;

3. the name, title, business address and business telephone number of the Privacy Officer who can answer questions and respond to complaints about the collection, use or disclosure of the information;
4. as appropriate, may include a written consent form to be signed/authorized by the person authorizing the collection, use, verification and disclosure of the information being collected; oral consent is also permissible.

Protection of Information

1. All employees, contracted agents, board members and volunteers with access to or knowledge of personal information retained by the Corporation will be required to sign a confidentiality agreement.
2. Member and director files (including information on databases) must be safeguarded against unauthorized access.
3. Member/director information must be stored in a locked filing cabinet. Secure storage facilities must be provided for archived member/director and accounting information.
4. Employees, contracted agents and members of the Board, where appropriate, should have access to records containing personal information only if required in order to fulfil their duties and only upon formal request to and approval by the Privacy Officer.
5. When communicating member issues to the Board, employees or contracted agents should use non-identifying information as much as possible. For example, outstanding membership dues reports should use codes in place of the actual names of members.
6. Databases containing files with personal information, and other confidential electronic files must be password protected against unauthorized access.
7. Screensavers or other protective action will be used to protect confidentiality of personal information on computer monitors.
8. All employees, contractors or other Corporate agents, including volunteers, have a responsibility to ensure that unauthorized individuals do not have unsupervised access to areas where files are kept and used.
9. Personal information will be disposed of at the end of the required storage period for member records and financial records of 7 years after the end of the fiscal year.
10. Paper-based personal information must be shredded prior to disposal. Electronic media must be purged prior to disposal.

Release of Information

No personal information will be released to third parties without the written consent of the individual. When responding to inquiries for references, employees or contracted agents should limit information provided to the questioner and confirm only the information already provided by the individual making the inquiry.

It is not necessary to have a signed consent to release information to an accountant appointed by the Corporation to perform an annual audit or to the manager of the Corporation's bank accounts.

Employees or contracted agents will take reasonable care to confirm the identity of the people to whom information is released.

Personal information will be released to the following:

1. Funders: The Corporation, in order to be in compliance with funding program requirements, may need to release information to funders and auditors. Individuals doing these jobs have their own professional code of ethics and are required to maintain confidentiality. Employees or contracted agents should confirm that the person concerned is seeking access legitimately.
2. Law Enforcement: While the Corporation has a responsibility to protect the rights of members and directors to privacy, this responsibility must be balanced with an obligation to the broader community. Law enforcement agencies requesting personal information about members, board members or volunteers, will be required to provide a written request or "warrant" before information will be released.

Personal information may be released to the police:

i. In the context of reporting criminal activity, employees or contracted agents with personal knowledge should report theft, damage or fraud;
ii. With respect to crimes against persons, witnesses are obligated to report and provide appropriate information to the police so that charges can be laid.

Access to and Correction of Personal Information

1. The Privacy Officer will respond to all requests for access to or correction of personal information.
2. An individual who provides satisfactory identification will be informed of the existence, use and disclosure of his or her personal information and will be given access to that information. The privacy of others' personal information must be protected when giving an individual access to his or her own personal information, either by removing documents from files naming others or by copying such documents and "blacking out" names to protect personal information.
3. If the Privacy Officer believes that releasing personal information to an individual would prejudice the mental or physical health or security of any person, he or she will not release the information.
4. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate. If the Privacy Officer is not in agreement with the individual's request for correction, a counter-statement will be filed with the original information.

Procedure for Handling Complaints

The Privacy Officer will respond to all complaints about collection, use, disclosure, storage and disposal of personal information within thirty days of the request being made, and advise the complainant as to the action that has been taken.

Each complaint will be assessed to determine whether:

1. Correction of personal information is necessary;
2. Information was collected, used, released or disposed of inappropriately;
3. The Corporation's policies and procedures need to be strengthened;
4. Disciplinary or other action needs to be taken with respect to a breach of a confidentiality agreement.

Where necessary, the Privacy Officer will make the necessary recommendations to the Board of Directors in connection with resolution of the complaint.

Breach of Confidentiality

It is a breach of confidentiality to:

1. Discuss any confidential information within or outside the organization where it may be heard by individuals who are not authorized to have access to that information;
2. Provide confidential information or records to unauthorized individuals;
3. Leave confidential information in written form or displayed on a computer terminal in a location where it may be viewed by unauthorized individuals.

A breach of confidentiality may be grounds for employees or contracted agents to be disciplined or terminated.

A breach of his or her confidentiality obligation may be grounds for a board member to be removed as a director of the corporation. A board member who breaches confidentiality may not be covered by the Corporation's insurance if he or she is sued for libel.

Contact Information:

To reach the Corporation's Privacy Officer

Email: inclusionontario@gmail.com

Telephone: 1-877-681-5128