

Immigrant Council for Arts Innovation (ICAI)

Personal Information Protection Policy

ICAI is committed to safeguarding the personal information entrusted to us by our members, volunteers, and employees. We manage your personal information in accordance with Alberta's Personal Information Protection Act and other applicable laws. This policy outlines the principles and practises we follow in protecting your personal information.

This policy applies to ICAI and to any person providing services on our behalf. A copy of this policy is provided to any member on request.

What is personal information?

Personal information means information about an identifiable individual. This includes an individual's name, home address, phone number, and educational or professional history.

What personal information do we collect?

We collect only the personal information that we need for the purposes of providing services to our clients, including personal information needed to:

- deliver requested services
- enroll a member in a program
- to send information regarding ICAI membership
- provide correspondence, newsletter, and other information regarding the organisation (ICAI)

We normally collect member personal information directly from our members. Most of the information is collected by email and google forms. We may collect your information from other persons with your consent or as authorized by law.

Website: No personal information is collected about general website visitors.

We inform our members, before or at the time of collecting personal information, of the purposes for which we are collecting the information. The only time we don't provide this notification is when a member volunteers information for an obvious purpose (for example, producing a credit card to pay a membership fee when the information will be used only to process the payment).

Consent

We ask for consent to collect, use, or disclose member personal information, except in specific circumstances where collection, use, or disclosure without consent is authorized or required by law.

We may assume your consent in cases where you volunteer information for an obvious purpose.

We assume your consent to continue to use and, where applicable, disclose personal information that we have already collected, for the purpose for which the information was collected.

We ask for your express consent for some purposes and may not be able to provide certain services if you are unwilling to provide consent to the collection, use, or disclosure of certain personal information. Where express consent is needed, we will normally ask clients to provide their consent orally (in person, by telephone), or in writing (by signing a consent form, or by email).

In cases that do not involve sensitive personal information, we may rely on “opt-out” consent. For example, we may disclose your contact information to other organizations that we believe may be of interest to you, unless you request that we do not disclose your information. You can do this by checking the appropriate box on our application form or by telephoning our local number/toll-free number.

A member may withdraw consent to the use and disclosure of personal information at any time, unless the personal information is necessary for us to fulfill our legal obligations. We will respect your decision, but we may not be able to provide you with certain services if we do not have the necessary personal information.

We may collect, use, or disclose client personal information without consent only as authorized by law. For example, we may not request consent when the collection, use, or disclosure is to determine suitability for an honour or award, or in an emergency that threatens life, health, or safety.

CASL Preference (Opt in/Unsubscribe)

ICAI believes that honesty is the best policy, and that applies to our electronic communications, too.

ICAI follows the Canadian Anti-Spam Legislation (CASL). This means that we need to have your permission to keep you up to date about services, helpful news or other relevant information. (Please see the Appendix -1 for checklist).

How do we use and disclose personal information?

We use and disclose members' personal information only for the purpose for which the information was collected, except as authorized by law. Information regarding members is collected to provide correspondence, newsletter, and other information regarding ICAI.

What is personal employee and board member information?

Personal employee information is personal information about an employee or volunteer which is collected, used, or disclosed solely for the purposes of establishing, managing, or terminating an employment relationship or a volunteer work relationship. Personal employee information may, in some circumstances, include a Social Insurance Number, a performance review, etc.

We can collect, use, and disclose your personal employee information without your consent only for the purposes of establishing, managing, or terminating the employment or volunteer relationship. We will provide current employees and volunteers with prior notice about what information we collect, use, or disclose and our purpose for doing so.

What personal employee and board member information do we collect, use, and disclose?

We collect, use, and disclose personal employee information to meet the following purposes:

- Determining eligibility for employment or volunteer work, including verifying qualifications and references
- Establishing training and development requirements
- Assessing performance and managing performance issues, if they arise
- Administering pay and benefits (paid employees only)
- Processing employee work-related claims (e.g. benefits, workers' compensation, insurance claims) (paid employees only)
- Complying with requirements of funding bodies (e.g. lottery grants)
- Complying with applicable laws (e.g. Canada Income Tax Act, Alberta Employment Standards Code)

We only collect, use, and disclose the amount and type of personal employee information that is reasonable to meet the above purposes. The following is a list of personal employee information that we may collect, use, and disclose to meet those purposes.

- Contact information such as your name, home address, and telephone number
- Criminal background checks
- Employment or volunteer information such as your resume (including educational background, work history, and references), reference information and interview notes, letters

of offer and acceptance of employment, policy acknowledgement forms, background verification information, workplace performance evaluations, emergency contacts, etc.

- Benefit information such as forms relating to applications or changes to health and insurance benefits including medical and dental care, life insurance, short and long-term disability, etc. (paid employees only)
- Financial information, such as pay cheque deposit information and tax-related information, including Social Insurance Numbers (paid employees only)
- Other personal information required for the purposes of our employment or volunteer relationship

We will inform our employees and volunteers of any new purpose for which we will collect, use, or disclose personal employee information, or we will obtain your consent, before, or at the time the information is collected.

What information do we provide for employment/volunteer references?

In some cases, after your employment or volunteer relationship with us ends, we will be contacted by other organizations and asked to provide a reference for you. It is our policy not to disclose personal information about our employees and volunteers to other organizations who request references without consent. The personal information we normally provide in a reference includes:

- Confirmation that an individual was an employee or volunteer, including the position, and date range of the employment or volunteering
- General information about an individual's job duties and information about the employee or volunteer's ability to perform job duties and success in the employment or volunteer relationship

How do we safeguard personal information?

We make every reasonable effort to ensure that personal information is accurate and complete. We rely on individuals to notify us if there is a change to their personal information that may affect their relationship with our organization. If you are aware of an error in our information about you, please let us know and we will correct it on request wherever possible. In some cases, we may ask for a written request for correction.

We protect personal information in a manner appropriate for the sensitivity of the information. We make every reasonable effort to prevent any loss, misuse, disclosure, or modification of personal information, as well as any unauthorized access to personal information.

We use appropriate security measures when destroying personal information, including shredding paper records and permanently deleting electronic records. All our files are stored in Google drive which are stored in secure, encrypted data centers. Some relevant contact information may be saved in Mailchimp servers; they also utilize secure and encrypted data centers in addition to strong internal security mechanisms. Correspondence from/to members and copies of contracts and other relevant correspondence are maintained in the Google drive.

We retain personal information only as long as is reasonable to fulfill the purposes for which the information was collected or for legal or business purposes.

Access to records containing personal information

Individuals have a right to access their own personal information in a record that is in the custody or under the control of ICAI, subject to some exceptions. For example, organizations are required under the Personal Information Protection Act to refuse to provide access to information that would reveal personal information about another individual.

If we refuse a request in whole or in part, we will provide the reasons for the refusal. In some cases where exceptions to access apply, we may withhold that information and provide you with the remainder of the record.

You may make a request for access to your personal information by writing to admin@icaionline.org designated to ensure compliance with PIPA. You must provide sufficient information in your request to allow us to identify the information you are seeking.

You may also request information about our use of your personal information and any disclosure of that information to persons outside our organization. In addition, you may request a correction of an error or omission in your personal information.

We will respond to your request as soon as possible.

Questions and complaints

If you have a question or concern about any collection, use, or disclosure of personal information by ICAI, or about a request for access to your own personal information, please contact admin@icaionline.org designated to ensure compliance with PIPA.

Appendix - 1

Canadian Anti-Spam Legislation (CASL)

Canada's anti-spam legislation (CASL) is the federal law dealing with spam and other electronic threats. It is meant to protect Canadians while ensuring that businesses can continue to compete in the global marketplace.

COMPLIANCE CHECKLIST

This list has been created to assist ICAI to ensure that they avoid sending unsolicited commercial electronic messages (CEMs).

- Analyze the messages that we send to identify any that constitute CEMs.
- Review existing mailing lists to flag any addresses for which you do not have consent to send a CEM. If necessary, remove these addresses from the mailing lists.
- Update mailing lists (whether these are electronic spreadsheets, databases, or Customer Relationship Management (CRM) systems) to include the following fields:
 - **For all consents:** Whether the consent was expressed or implied.
 - **For express consents:** The date the consent was given; and the documentation (e.g. signed form) that proves that the consent was granted.
 - **For implied consents:** The manner that the implied consent was granted (e.g. business relationship); your proof of consent (e.g. a contract signed by the individual for consulting work); the date the consent came into effect; and the expiry date of the consent.
- Ensure that ICAI has a system in place (preferably automated) to ensure that all future consents and unsubscribe requests are promptly recorded in your mailing lists and that these are effective to prevent you from sending unwanted CEMs.
- Ensure that all of your requests for consent contain the required information (identification and unsubscribe option).
- Ensure that all of your CEMs contain the required information (purpose, identification and unsubscribe option).
- Train all relevant contractors on CASL's requirements and the processes ICAI has in place to comply with those requirements.

Date Approved: Feb 2, 2022