



PLAN INTERNATIONAL CANADA PRIVACY POLICY

1. INTRODUCTION

Plan International Canada (“we”, “our”, or “us”) is committed to protecting the privacy and security of Personal Information under its control about its donors, sponsors, children, website visitors, employees, volunteers, interns and others whose Personal Information it collects (“you” or “your”).

This Policy sets out the minimum standards in relation to our collection, use, disclosure, retention, protection, and disposal of Personal Information. This Policy will continue to evolve to reflect current best practices in privacy and data protection and changes in our organizational practices or legal and regulatory requirements. We encourage you to periodically check our website for updates to this Policy.

Personal Information means information relating to an individual which is personally identifiable, or for which it is reasonably foreseeable in the circumstances could be utilized, either alone or with other information to identify an individual.

Personal Information does not include anonymous or aggregate information that cannot be tracked back to you personally. For example, we may use aggregate data to improve the quality and efficiency of our products and services, and to enhance our marketing efforts.

2. STATEMENT OF PURPOSE

The purpose of this Policy is to ensure that:

- we uphold the privacy rights of all individuals (“**data subjects**”) that we engage with, with special emphasis on the Personal Information of children, program participants, and their families;
- any Personal Information to which this Policy applies is appropriately collected, used, disclosed and maintained; and
- only authorized individuals can access Personal Information.

To maintain appropriate standards of care in managing Personal Information, we commit to the 10 principles outlined in the Canadian Standards Association’s *Model Code for the Protection of Personal Information* (CSA *Model Code*). The *Model Code*, which was recognized as a national standard for privacy protection in 1996, is used across Canada as the basis for personal information legislation, policies and procedures including the federal privacy law for the private sector, the *Personal Information Protection and Electronic Documents Act* (PIPEDA). The 10 principles of the *Model Code* are:

1. Accountability
2. Identifying Purposes
3. Consent
4. Limiting Collection
5. Limiting Use, Disclosure and Retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual Access
10. Challenging Compliance

3. PRIVACY PRINCIPLES

PRINCIPLE 1: ACCOUNTABILITY

We accept full responsibility for the Personal Information under our control. We have established internal procedures to comply with this Policy and have designated a Chief Privacy Officer to be accountable for compliance with the following principles.

- 1.1 Responsibility for ensuring compliance with the provisions of this Policy rests with our Chief Privacy Officer. The Chief Privacy Officer may delegate responsibilities to other employees to oversee privacy compliance.
- 1.2 We use contractual and other commercially reasonable means to ensure that any third parties with access to Personal Information entrusted to us provide a comparable level of protection while such information is being processed by them.
- 1.3 This Policy is regularly reviewed to ensure that it reflects privacy best practices and current legislation.
- 1.4 In addition to this Policy, we have:
 - developed and implemented practices to protect Personal Information.
 - established procedures to receive and respond to privacy inquiries or complaints from data subjects, as well as manage privacy breaches.
 - established a privacy training and awareness program for our employees that highlights Personal Information protection responsibilities, with special emphasis on the protection of the Personal Information of children, program participants and their families.
 - committed to building data privacy into processes, systems, projects or work activities that may impact the privacy of Personal Information entrusted to us. We assess these during the design phase of this work and at the time of substantial modifications involving Personal Information.

PRINCIPLE 2: IDENTIFYING PURPOSES

We collect Personal Information for specific purposes and identify these purposes at or before the time the information is collected.

- 2.1 We collect Personal Information from data subjects and may use it for the following lawful purposes, including, without limitation:
 - to understand the needs of individuals and respond to requests for information, products or services;
 - to verify an individual's identity;
 - to complete a financial transaction such as the sponsorship of a child;
 - to provide appropriate levels of service following completion of a transaction, such as a change in banking or credit card information, or a change in sponsorship or donations;
 - to establish relationships, provide support, as well as communicate updates, marketing and promotional materials, or other news;
 - to personalize and improve your experience including by conducting satisfaction surveys, tailoring advertising outputs, and reviewing aggregated data reports;
 - to administer employees, volunteers, speakers, other contributors and any associated activities; and
 - to meet legal or regulatory requirements imposed upon us from time to time.

2.2 Unless otherwise permitted or required by law, we collect and use the minimum amount of Personal Information necessary for the purposes identified in section 2.1.

2.3 Upon request, we shall explain the purposes for which such information will be used or refer the requestor to another representative who can explain the purposes.

PRINCIPLE 3: CONSENT

We obtain informed consent for the collection, use or disclosure of Personal Information, except where inappropriate.

3.1 Unless otherwise permitted or required by law, we shall not use or disclose existing Personal Information for any new purpose that is not outlined in section 2.1 without first identifying and documenting the new purpose and obtaining the individual's consent.

3.2 Consent can be obtained in person, by phone, by mail, or via the Internet (e.g., ticking a box). Consent is only implied or assumed if the collection, use or disclosure of Personal Information is obvious based on the individual's actions or inactions and the Personal Information is non-sensitive in nature and context.

3.3 We will only require individuals to consent to the collection, use or disclosure of Personal Information as a condition to the supply of a product or service if it is required to fulfil the identified purposes, e.g., supplying a credit card number to process a sponsorship application.

3.4 By providing your Personal Information to us, this means that you agree to our collection, use and disclosure of your Personal Information in accordance with this Privacy Policy. If you do not agree with these terms, please do not provide your Personal Information to us.

3.5 If an individual provides us or our service providers with Personal Information about another person, it is their responsibility to obtain consent from such person to enable us to collect, use and disclose such information for the purposes set forth in this Policy.

3.6 A data subject may withdraw their consent at any time, subject to legal or contractual restrictions and reasonable notice. For example, you are always given the ability to opt-out of receiving promotional electronic messages from us by using the available "unsubscribe" link. We will inform data subjects of the implications of withdrawing consent, as we may be limited or unable to provide information, products or services as a result.

3.7 In order to protect the Personal Information of children and young people involved in our activities, we take extra precautions including the following:

(i) we ensure that information provided to a child or young person about processing their Personal Information is concise, easily accessible, and uses clear and plain language.

(ii) we ensure that the child or young person's parents or guardians provide consent where appropriate, and in accordance with our [Safeguarding Policy](#).

(iii) we ensure that all our employees and third parties involved in collecting and processing the Personal Information of children and their families understand the sensitivity of this information, and that they only use it for its specific intended purposes.

3.8 In certain cases, we may have Personal Information in our records about individuals who are now resident in Quebec, the European Union, or the United Kingdom. In such cases, we have taken steps to ensure that we are compliant with any obligations that we may have under the *Act to Modernize Legislative*

Provisions respecting the Protection of Personal Information (Law 25), the General Data Protection Regulation (GDPR) (EU 2016/679) and relevant UK Privacy Law.

PRINCIPLE 4: LIMITING COLLECTION

We limit the collection of Personal Information to what is necessary for the identified purposes. Personal Information is collected by fair and lawful means.

4.1 Our business units are responsible for ensuring that all information collected is limited, both in amount and type, to what is needed to fulfill the identified legitimate organizational purposes.

4.2 In most cases, Personal Information is collected directly from the data subject.

4.3 With the data subject's authorization or where permitted or required by law, we may also collect Personal Information from references, financial institutions, credit reporting agencies or other third parties.

PRINCIPLE 5: LIMITING USE, DISCLOSURE AND RETENTION

We do not use or disclose Personal Information for purposes other than those for which it is collected (See Principle 2.2), except with the consent of the individual or as required by law.

We retain Personal Information only as long as necessary to fulfil those purposes, or as required by law.

5.1 **Disclosure for investigations, law enforcement.** There are circumstances where a disclosure without consent is justified or permitted, for example in the context of a legal investigation or a request from law enforcement authorities, or where we believe, upon reasonable grounds, that the disclosure is necessary to protect the rights or safety of an identifiable person or group.

5.2 **Transfers to Third-Party Service Providers.** Your Personal Information may also be shared with third party service providers who assist us in establishing, managing or maintaining our relationship with you. These organizations, such as banking institutions, credit agencies, our media partners, as well as contractors who perform various functions to provide or assist in the delivery of services including the dissemination of marketing and promotional materials, commit to safeguarding your Personal Information. In these cases, we ensure that appropriate controls are in place before disclosing Personal Information. These controls include:

- putting contracts in place that specify the reason for collection and use, identify the service provider's privacy responsibilities related to the services provided, and ensuring secure transfer and maintenance of the transferred information. We ensure that these agreements are in place before any access is granted to your Personal Information.
- ensuring that the service provider returns or destroys the transferred Personal Information upon our request.
- ensuring that the service provider does not forward the transferred Personal Information to third parties without our written permission.
- confirming that the service provider maintains reasonable administrative, technical and physical safeguards that are designed to ensure the confidentiality, integrity and security of the transferred Personal Information.

5.3 **Transfers to Third-Party Service Providers outside of your province of residence and/or Canada.** Your Personal Information may be transferred outside of your province of residence and/or Canada to be processed or stored by us or our service providers, including data hosting providers. This information may be provided to law enforcement or national security authorities of that jurisdiction upon request, in order to comply with foreign laws. Before we make this transfer, we ensure that appropriate safeguards are put in place so that our privacy standards will be maintained by these third

parties.

5.4 We do not and will never sell any Personal Information to third parties for marketing or any other commercial purposes.

5.5 Personal Information may be shared between Plan International related companies, such as the Plan International Head Office in England, for internal audit, management, billing, promotional or administrative purposes including defending and bringing legal actions.

5.6 We retain Personal Information only for as long as it is deemed necessary, to fulfil the purposes identified in Principle 2.1 or as required by law. The retention period may extend beyond your relationship with us for legitimate business reasons.

5.7 Personal Information that is no longer necessary or relevant for the identified purposes or no longer required to be retained by law is securely destroyed, erased or made anonymous. You have the right to request that we erase your Personal Information when it is no longer required for the purposes for which it was collected or if you think it has been used unlawfully.

PRINCIPLE 6: ACCURACY

We make reasonable efforts to keep Personal Information as accurate, complete and up-to-date as is necessary to fulfil the purposes for which the information is to be used.

6.1 We rely upon the individuals who provide us with their Personal Information to ensure its accuracy and completeness.

6.2 We have established internal procedures to preserve the integrity of the Personal Information received by individuals in accordance with reasonable commercial standards.

6.3 We will update a donor's Personal Information as required to fulfil the identified purposes, or upon notification by the donor.

PRINCIPLE 7: SECURITY SAFEGUARDS

We protect Personal Information with security safeguards appropriate to the sensitivity of the information.

7.1 We protect Personal Information against a variety of risks such as loss, theft or unauthorized access, disclosure, copying, use, modification or destruction by using appropriate security measures.

7.2 These safeguards applied to Personal Information depend on many factors including the available technology, the type, scope, context and purpose of processing as well as the sensitivity of the information.

Safeguards include physical, organizational and technical measures such as:

- security card access to our premises.
- restrictions on employee access to files on a “need to know” basis consistent with the roles and responsibilities assigned to the employee.
- locking up Personal Information as necessary, so that it is not left unattended in plain view.
- implementing privacy protection provisions for our employees working remotely.
- firewalls, anti-malware detection software, strong passwords and software solutions for technical security (including ensuring that information is only collected on Plan websites via a secure, 256-bit encrypted Secure Socket Layer session).

7.3 Our employees with access to Personal Information are required, as a condition of employment, to safeguard Personal Information in their care. Employees sign confidentiality agreements and must complete annual privacy awareness training.

7.4 Where required by applicable law, we notify the relevant privacy authority and data subjects whose Personal Information was involved in a security incident.

PRINCIPLE 8: OPENNESS

We make readily available specific information about our privacy management policies and practices to individuals upon request.

8.1 This information includes:

- a) the name, title and address of the Chief Privacy Officer to whom inquiries or complaints can be forwarded;
- b) the means of gaining access to your Personal Information held by us, including a Privacy Access, Inquiries and Complaints Procedure, Breach Management Procedure, and a Breach Reporting Form (available in both English and French languages);
- c) a description of the type of Personal Information held by us, including a general account of its use and disclosure; and
- d) a copy of this Policy or other information that explains our information handling practices.

8.2. We make information available to help individuals exercise choices regarding the use and disclosure of their Personal Information upon request. Our employees are able to answer inquiries about our information handling practices and to refer unanswered questions or privacy complaints to our Chief Privacy Officer.

PRINCIPLE 9: INDIVIDUAL ACCESS

We inform individuals of the existence, use and disclosure of their Personal Information upon request, and gives the individual access to their information. Individuals are given the opportunity to challenge the accuracy and completeness of their information and have it amended or deleted as appropriate.

9.1 Upon written request, we will provide data subjects a reasonable opportunity to review their Personal Information as contained in our files, whether in electronic or in paper form. The written request must provide sufficient detail so that we can properly and efficiently locate the records requested.

9.2. Upon request, we will provide an account of the use and disclosure of the individual's Personal Information and, where reasonably possible, will state the source of the information.

9.3 In order to safeguard and prevent fraudulent access to Personal Information, we will take reasonable steps to verify the identity of a requestor, or their legally authorized representative, before granting them with access to their file.

9.4 We will respond to access requests within 30 days of receipt of the request or as otherwise prescribed by relevant legislation.

9.5 Individuals will be provided with any assistance required to access or understand their Personal Information, including clarifying exactly what they are looking for or receiving in response to their access request.

9.6 Depending on the amount of information requested, there may be a nominal fee charged to cover any costs associated with responding to the request. We will inform the individual of any such fees prior to fulfilling the access request.

9.7 We shall promptly correct, complete, or delete any Personal Information that is successfully demonstrated to be inaccurate, incomplete, or lawfully subject to erasure. If we do not agree with the individual regarding a correction or completeness of information, this shall be noted in the individual's file. Where appropriate, we shall transmit to third parties having access to the disputed Personal Information, any disagreement that we have with the individual about the accuracy of the information.

9.8 An individual's right to access, correct, or request deletion of Personal Information is subject to applicable legal restrictions. If we do not have custody of the Personal Information requested or must decline to provide an individual with access to their Personal Information for legal, regulatory or other reasons, an explanation will be provided when permitted.

PRINCIPLE 10: CHALLENGING COMPLIANCE

An individual shall address a challenge concerning our compliance with the principles set out in this Privacy Policy to the Chief Privacy Officer.

10.1 We have procedures in place to receive, investigate, respond to and track concerns or complaints about our management of Personal Information.

10.2 Upon conclusion of a complaint investigation, the Chief Privacy Officer will inform the complainant of:

- a) the results of the investigation; and
- b) any appropriate remedy or corrective action we will undertake to address the complaint, including if necessary, amending Plan's policies and procedures.

4. RESPONSIBILITIES

Implementing and maintain strong data privacy practices is an organization-wide imperative for Plan International Canada.

- 4.1 Our employees and volunteers are responsible for the protection of Personal Information and for complying with this Policy when processing Personal Information in connection with their work or volunteer activities.
- 4.2 Our People Leaders are responsible for ensuring that employees, volunteers and third-party service providers engaged with their teams are aware of and abide by this Policy.
- 4.3 The Chief Privacy Officer is responsible for ensuring compliance with this Policy.

5. QUESTIONS

Questions or concerns relating to Plan International Canada's Privacy Policy or requests related to our management or deletion of your Personal Information, including any privacy complaints, should be directed to:

Plan International Canada Inc
245 Eglinton Ave. East, Suite 300, Toronto, ON M4P 0B3

Attention: Pamela Spencer, General Counsel and Chief Privacy Officer
Phone #: 1-800-387-1418

Email: privacyoffice@planCanada.ca

APPENDIX: WEBSITE PRACTICES]

USAGE TRACKING

Our websites may automatically record some general information about your visit in order for us to engage in web statistical analysis using a web analytics service. We want to make sure our sites are useful to visitors, and ensure we engage in targeted advertising responsibly, such that customers receive information that is relevant to their needs and interests. User information gathered may include the:

- Internet domain for your Internet service provider, such as “company.com” or “service.ca” and the IP address of the computer you are using to access Plan’s website;
- Type of browser you are using, such as Internet Explorer, Firefox or Chrome;
- Type of operating system you are using such as Windows or Macintosh;
- Date and time of the visit to our site, the pages of our site that were visited, and the address of the previous website you were visiting if you linked to us from another website;
- Age category, gender, and affinity interests as determined by demographic and interest reports available through Google Analytics.

We make no effort to personally identify you based on your visit to our site. If you wish, you may opt out of being tracked by a web analytics service by disabling or refusing cookies; by disabling JavaScript within your browser; or by using the web analytics organization’s opt out service, for example, for Google Analytics, get the [Google Analytics Opt-Out Browser Add-On](#).

Data collected for web analytics purposes may be processed in any country where the web analytics organization used operates servers, and thus may be subject to the governing legislation of that country.

COOKIES

We also use "cookies" that identify you as a return visitor which can help us tailor information to suit your individual preferences, including but not limited to managing your donor shopping cart and checkout process, and maintaining your language settings. A cookie is a small text file that a website can send to your browser, which may then store the cookie on your hard drive. The goal is to save you time next time you visit, provide you with a more meaningful visit, and measure website activity. Cookies in and of themselves cannot be used to reveal your identity. Many browsers, however, allow you to disable cookie collection if you wish, or inform you when a cookie is being stored on your hard drive.

TARGETED ADVERTISING:

As you interact with our websites, third party advertising partners may use cookies, tracking pixels, web beacons and similar technologies to identify you as a visitor to our websites, and present you with targeted ads to help promote Plan International Canada. You can opt-out of the use of your information for select ad targeting by visiting this site: <http://youradchoices.ca/choices>, and also by setting up “Do Not Track” options available through your browser. We also occasionally provide your Personal Information to trusted advertising partners for the purpose of presenting you with targeted ads on behalf of Plan International Canada. You can request that your Personal Information not be shared

with our advertising partners by contacting our Chief Privacy Officer at the contact info provided below.

1. [OTHER IMPORTANT NOTES REGARDING OUR WEB PRACTICES](#)

[**EXTERNAL LINKS**](#)

We are not responsible for any third-party websites which may be accessible through links from this website. If you follow a link to any of these third-party websites, they will have their own privacy policies and you will need to check these policies before you submit any Personal Information to them.

[**THIRD-PARTY SOCIAL MEDIA**](#)

Plan International Canada's use of social media serves as an extension of our presence on the Internet. Social media account(s) are public and are not hosted on our servers. Users who choose to interact with Plan International Canada via social media should read the terms of service and privacy policies of these third-party service providers and those of any applications used to access them.

We may offer you the opportunity to engage with our content through third-party social networking websites and applications. When you engage with our content this way, you may allow us to have access to certain information associated with your social media account (e.g. name, username, e-mail address, picture) to deliver the content or as part of the website or application. We may use this information to confirm your identity and to personalize your experience.

[**SPECIAL NOTE FOR PARENTS**](#)

Plan International Canada websites are not directed at children, and we request that children under the age of 13 not provide Personal Information through our sites. If the website user is under the age of 13, parental consent must be sought before Personal Information may be provided on behalf of that user.

[**SECURITY**](#)

No method of transmitting or storing data is 100% secure. As a result, although we strive to protect your Personal Information, we cannot guarantee the security of any information you transmit to us through or in connection with Plan International Canada websites. If you have reason to believe that your interaction with us is no longer secure (for example, if you feel that the security of any account you might have with us has been compromised), you must immediately notify us of the problem in order for Plan International Canada to resolve the issue in a timely manner. Also keep in mind that e-mail is not a secure form of communication so never send sensitive Personal Information to us via e-mail.