Policy: Privacy Policy
Sub-section: Finance
Date of last Review: New Policy
Date of last Approval: June 25, 2024

1. Purpose

The purpose of this policy is to:

- Define Personally Identifiable Information (PII) and establish standards for how PII must be collected, maintained, stored, and destroyed by CPC staff, contractors, vendors, and partners.

2. Inclusion, Diversity, Equity & Accessibility

This policy has been assessed for any implications it may have on inclusion, diversity, equity, and accessibility.

3. Scope of Policy

This policy covers all activities and services at Canadian Paralympic Committee.

4. Responsibilities

The Board of Directors is responsible for:

4.1 Establishing and approving policies and guidelines

4.2 Ensuring alignment of privacy practices with legal and regulatory requirements

The FAR Committee is responsible for:

4.3 Reporting to the Board on CPC's privacy performance and compliance

4.4 Assessing and managing privacy-related risks

Senior Leadership is responsible for:

4.5 Establishing, implementing and maintaining good privacy practices throughout the organization including leading by example

4.6 Providing necessary resources for appropriate measures and overseeing compliance with the policy

4.7 Providing regular privacy training to employees

4.8 Ensuring that contracts with vendors include privacy and security requirements

Employees are responsible for:

4.9 Adhering to established privacy guidelines and procedures

4.10 Reporting potential privacy concerns or incidents promptly

4.11 Using strong passwords, encryption and secure channels for data transmission

5. Definitions

5.1 **Personally Identifiable Information (PII)** includes any factual or subjective information, recorded or not, about an identifiable individual. This includes information in any form, such as:

- age, name, address, phone number, postal code, ID numbers, income, ethnic origin, or blood type;
- opinions, evaluations, comments, social status, or disciplinary actions; and
- employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions (for example, to acquire goods or services, or change jobs).
- Any type of medical data

6. Limitations

7. Content of Policy

7.1 PII Collection

PII is not to be collected by CPC staff, contractors, vendors, or partners unless there is a clear operational requirement to do so. Any collection of PII data collection outside of operational requirements must be approved by the Senior Leadership Team before PII collection can commence.

7.2 PII Storage and Maintenance

PII must be encrypted using at least 128-bit encryption at all times when it is in transit and at rest. System or database access to PII must be restricted only to authorized users, only for the time period during which their activities require access to PII. Any systems that provide access to PII must be secured with multi-factor authentication (MFA) and will be subject to quarterly access audits.

7.3 Right to be Forgotten

CPC will maintain the ability to provide individuals with the "right to be forgotten". CPC will maintain a process for processing requests by individuals to have their PII completely purged from CPC systems. CPC will make the details of the process available to the public via the Privacy Policy.

7.4 Destruction

If storing PII no longer serves the required operational purpose it was initially collected to meet, it will be destroyed. The data may be retained in an aggregated format.

7.5 Any violations of this policy as a whole, or in part, may result in disciplinary action which may include, but not be limited to, termination of employment or contract and/or such other legal actions as may be warranted in the circumstances. Refer to CPC's Disciplinary Policy for more information.

8. Associated Documents/Records

IM and IT Policies
Risk Management Policy

9. Revision History