SPORT DISPUTE RESOLUTION CENTRE OF CANADA

SDRCC

# Protection of Privacy Policy

**Final Version**

Adopted by resolution of the Board of Directors, February 24, 2017.

Revised by resolution of the Board of Directors, June 15, 2022; effective June 20, 2022.

# PROTECTION OF PRIVACY POLICY

**SDRCC**

1080 Beaver Hall Hill

Suite 950

Montreal, QC Canada

H2Z 1S8

Telephone:

1-866-733-7767 (toll-free)
1-514-866-1245 (local)

Fax:

1-877-733-1246 (toll-free)
1-514-866-1246 (local)

Website: www.sdrcc.ca

# Table of Contents

# Executive Summary

The Sport Dispute Resolution Centre of Canada (the “Centre”) Protection of Privacy Policy (“the Policy”) is based on the ten principles outlined in the **Model Code for the Protection of Personal Information** of the Canadian Standards Association and in the *Personal Information Protection and Electronic Documents Act*’s (“PIPEDA”) fair information principles: *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*.

The model was adapted in this Policy to combine principles 1 and 8 in a principle of Accountability and Openness, as well as to combine principles 4 and 5 into a general principle of Limiting Information, resulting in eight sections.

Section 1 – **Accountability and Openness**, designates a privacy officer responsible for compliance and enforcement and provides for information regarding specifics of the Policy and the related practices of the Centre to be easily accessible.

Section **2 - Identifying Purpose**, establishes that the purpose of any information collected will be identified at or before the time of collection.

Section **3 - Consent**, is to provide a definition of consent, as well as the valid types and withdrawals of consent.

Section 4 - **Limiting Collection and Use**, establishes a principle of limiting the collection, use, disclosure and retention of information to only what is reasonable and necessary for the purposes of the Centre.

Section 5 – **Accuracy**, is to ensure that the information obtained will be as accurate and up to date as possible.

Section 6 - **Safeguards and Security**, is to establish the methods and principles of the Centre to ensure proper measures are in force for the safety and security of information, including storage, destruction, retention, access, and Third Party protections and safeguards.

Section **7 - Individual Access**, is to provide the right of individuals to access, and change (where possible) their personal information on record with the Centre.

Section **8 - Challenging Compliance**, is to establish a principle of allowing for individuals to challenge any compliance issues they feel exist with the Policy.

# Introduction

The Centre is committed to respecting the privacy and confidentiality of all Personal Information gathered in administering its programs. The present Policy describes the way in which the Centre will adhere to and promote accountable Personal Information management practices in a manner that is consistent with applicable legislative and regulatory privacy requirements.

## A. Purpose

The Policy establishes how the Centre collects, uses, and discloses Personal Information during the course of its activities by providing principles for the management of Personal Information while ensuring optimal balance between the need of Personal Information to conduct the Centre's operations, the right to privacy of its clients, Employees, Board Members and stakeholders and other fundamental rights in accordance with the principle of proportionality.

## B. Scope

The Centre shall at all relevant times and in all of its operations comply with applicable federal, provincial and territorial privacy legislation and their regulations ("applicable privacy legislation"), as may be amended from time to time. It shall also comply with the *International Standard for the Protection of Privacy and Personal Information*, as published and amended from time to time by the Word Anti-Doping Agency in managing its Doping Tribunal and Doping Appeal Tribunal.

## C. Application

The Policy applies to all of the Centre's Employees, Board Members, Dispute Resolution Professionals, as well as to any Third Party engaged by the Centre.

## D. Amendments

The Policy may be updated or modified from time to time by the Centre's Board of Directors for any reason, including to account for the introduction of new technologies, business practices, stakeholder needs or applicable laws and regulations.

## E. Disclaimer

While the procedural rules governing the conduct of its dispute resolution services provide for confidentiality safeguards, as outlined in the *Canadian Sport Dispute Resolution Code* and/or the *OSIC Confidentiality Policy* (as applicable), the Centre cannot be held responsible for the conduct of the parties, Authorized Representatives or witnesses involved in dispute resolution proceedings (or in any Complaint procedures of the OSIC) which may cause unlawful disclosure of Personal Information that forms part of the evidentiary record before the Centre.

In delivering most of its services virtually, the Centre shall take reasonable steps to prevent unauthorized access to Personal Information in electronic form while stored on its own servers, however it cannot be held responsible for any breach caused by email or Internet service providers of intended email recipients.

The Centre's websites, including those of the OSIC and of Abuse-Free Sport, provide links to Third Party websites. The Centre is not responsible for the collection, use or disclosure of Personal Information obtained by those Third Party websites. It is strongly recommended that the Centre's website visitors consult the privacy policies of those Third Parties before disclosing any Personal Information.

## F. Definitions

*Authorized Representative:* any lawyer appearing before the Tribunal on behalf of the Individual, any other person so designated in writing by the Individual, or, in the case of a minor Individual who is not emancipated, any parent, legal guardian or authorized representative;

*Board Member:* any member of the Board of Directors of the Centre, as may be appointed from time to time by Canada's minister responsible for sport;

*Case Management Portal:* the proprietary online platform used by the Centre's Employees in the management of Tribunal proceedings to share information and documents with Dispute Resolution Professionals, Parties and their Authorized Representatives;

*Complaint:* a submitted complaint intake form, the receipt by the OSIC of information expressly deemed by the OSIC to constitute a complaint, or a complaint initiated by the OSIC, in each case regarding an alleged violation of the UCCMS;

*Complaint Management Portal:* the online platform used by the Centre's Employees and OSIC Professionals in the management of Complaints to share information and documents with the Director of Sanctions and Outcomes, Dispute Resolution Professionals, Parties and their Authorized Representatives;

*Dispute Resolution Professional:* any member of the Centre's roster of mediators and arbitrators acting upon appointment by the Centre or by consent of the Parties;

*Employee:* any person hired by the Centre to execute tasks in the conduct of its operations in exchange for monetary compensation or co-op education credits. For the sake of clarity, a Dispute Resolution Professional is not an Employee;

*Express Consent:* consent given electronically, in writing or orally when necessary by an Individual, which must always be unequivocal and not require inference on the part of the Centre;

*Implied Consent:* consent that can be reasonably inferred from an Individual's actions or inaction;

*Individual:* a person whose Personal Information is collected, used, disclosed or retained by the Centre;

*OSIC:* Office of the Sport Integrity Commissioner, an independent function within the Centre, responsible to administer and enforce the UCCMS;

*OSIC Professional:* any member of the Centre's roster of OSIC independent investigators acting upon appointment by the Centre;

*Party:* user of the Centre's dispute resolution services or OSIC services including, but not limited to, a claimant, a respondent, an affected party or an intervenor as defined in the *Canadian Sport Dispute Resolution Code* or other OSIC policies and procedures;

*Personal Information:* information about an identifiable Individual, excluding information otherwise publicly available;

*Privacy Officer:* the Centre's Director of Operations or any other Board Member or Employee that the Board of Directors may nominate from time to time;

*Request:* right of the Individual to access and ask for the correction of his/her Personal Information as well as a demand, by any person, to access information other than his/her Personal Information (access Request);

*Sensitive Personal Information:* more delicate Personal Information such as, but not limited to Personal Information relating to an Individual's racial or ethnic origin, commission of offences (criminal or otherwise), health and genetic information;

*Service User:* any person providing Personal Information to the Centre for the purpose of receiving services or taking part in a Centre's program other than the Tribunal services, such as but not limited to, registrants to events held by the Centre, applicants to the roster of Dispute Resolution Professionals, applicants to the Board of Directors and applicants for employment and internship positions.

*Third Party:* any person, institution, corporation or other entity that has entered into contractual agreements with the Centre in the conduct of its operations to provide services which involve access or potential access to Personal Information including, but not limited to, investigators, Abuse-Free Sport Helpline operators, consultants, and other suppliers or service providers. For the sake of clarity, the definition of a Third Party excludes Dispute Resolution Professionals;

*Tribunal*: Dispute Resolution Secretariat of the Centre;

*UCCMS*: Universal Code of Conduct to Prevent and Address Maltreatment in Sport (UCCMS), available here.

# 1 - Accountability and Openness

## 1.1 Privacy Officer

a) The role of the Privacy Officer is to ensure that the Policy complies with applicable privacy laws and regulations, to monitor the Centre's compliance with the Policy, and to report and respond to privacy complaints and breaches.

b) The Privacy Officer oversees the implementation of the Centre's other policies and procedures which also contribute to the protection of Personal Information.

c) The Privacy Officer may be contacted by email at priv@crdsc-sdrcc.ca or by calling the Centre's main office telephone number or in person or by mail at

1080, côte du Beaver Hall, Bureau 950
Montréal (Québec)
H2Z 1S8.

d) In the absence or incapacity of the Privacy Officer, or at any time deemed necessary, the Centre's Board of Directors shall designate a Board Member or Employee to replace the Privacy Officer.

## 1.2 Publication of the Policy

a) The Policy shall be made publicly available through the Centre's website(s) and upon request.

b) The Centre shall make accessible, through the Policy or otherwise:

   i. A description of the type and purpose of Personal Information gathered;

   ii. The methods for Individuals to gain access to their Personal Information on the Centre's records; and

   iii. Where Personal Information is shared with Third Parties, a justification for giving access to those Third Parties.

## 1.3 Amendments

a) Amendments to the Policy shall be made publicly available, after their adoption but at least one (1) month prior to becoming effective, through the Centre's website or upon request. It is recommended to Individuals sharing Personal Information with the Centre to check the Policy regularly for changes and updates.

## 1.4 Discrepancies

a) In the event that there are any discrepancies between applicable privacy legislation and the Policy, the applicable privacy legislation shall take precedence.

# 2 - Identifying Purpose and Type of Information Collected

## 2.1 Types of Information Collected

a) The Centre collects Personal Information that is necessary for its operations and/or required by law.

b) The Centre's operations minimally require last names, given names, and contact information (email address, telephone number and mailing address) of Service Users, Parties and, if applicable, their Authorized Representatives.

c) The Centre is also seized by the Parties or their Authorized Representatives of certain Personal Information and/or Sensitive Personal Information through the evidentiary record and submissions filed in the course of dispute resolution proceedings, through the Complaint management process or administration of the UCCMS, such as health information, criminal offences, last name, given name, contact information, and information relating to complaints against individuals and related sanctions. Personal Information provided by the Parties or their Authorized Representatives, including without limitations, financial information, health information, last name, given name and contact information, information regarding Complaints or other information about procedures before the Centre, may also be collected in order to determine the admissibility to certain programs offered by the Centre (e.g. legal aid, mental health referrals) and in order to offer such programs to the eligible Parties.

d) The Centre collects Personal Information from its Employees, Board Members and Dispute Resolution Professionals which includes, but is not limited to financial information, last names, given names and contact information.

e) The Centre's Case Management Portal and the OSIC Complaint Management Portal collect cookies on user accounts such as IP addresses, sections of portal visited, and information downloaded.

f) The Centre's websites also collect non-identifiable information such as cookies including, but not limited to, IP addresses, sections of website visited, and information downloaded.

### 2.2 Purpose

a) The purposes for which Personal Information is collected by the Centre are enumerated in Appendix A.

b) The Centre will inform the Individual of the applicable purposes at or before the time that the Personal Information is collected and used.

## 3 – Obtaining Valid, Informed Consent

### 3.1 When to Seek Consent

a) Except when it is reasonable to think that implicit consent was given, in case of emergency or when not required by law, the Centre must obtain valid consent from the Individual, or Authorized Representative, at or before the time of collection for the use and disclosure of Personal Information.

b) Except when permitted by law, if the Personal Information collected is to be used for purposes not originally agreed upon by the Individual, the Centre will notify and obtain consent for any new purposes for which it intends to use such information.

### 3.2 Express and Implied Consent

a) Consent can either be Express Consent or Implied Consent and may be provided by the Individual or by an Authorized Representative. In determining the form of the consent required, the Centre will take into account the sensitivity of the Personal Information and the reasonable expectations of the Individual. Notwithstanding the above, except when permitted by law, the Centre shall seek Express Consent when the Personal Information is likely to be considered sensitive.

### 3.3 Withdrawal of Consent

a) An Individual may withdraw his or her consent at any time, on reasonable notice, subject to legal or contractual restrictions. The Centre shall inform the Individual of the implications of such a withdrawal, which may result in forfeiture of certain services or information.

# 4 – Limiting Collection and Use

## 4.1 Collection

a) The Centre shall only collect Personal Information by fair and lawful means necessary for the identified purposes.

## 4.2 Use and Disclosure

### 4.2.1 General Principle

a) The Centre shall only use and disclose Personal Information for the identified purposes and such purposes shall be limited solely to fulfilling the necessary functions of the Centre.

### 4.2.2 Applications of the Principle

a) Personal Information described in section 2.1 b) may be shared with other Parties involved in the same dispute or Complaint and with their Authorized Representatives during the proceedings.

b) Personal Information described in section 2.1 c) may, at the sole discretion of the OSIC in accordance with OSIC policies and procedures and/or by any OSIC Professional in the course of an investigation, or at the sole discretion of the Dispute Resolution Professional appointed to hear a case, be disclosed in the investigation report and/or arbitral awards when necessary to provide reasoning for the decisions rendered.

c) Any Personal Information described in section 2.1 c) that is disclosed in a decision of the Doping Tribunal and that allows for the identification of an Individual against whom a doping violation has been asserted shall be redacted after 10 years of the decision date

d) Personal Information described in section 2.1 d) shall be used strictly for purposes of human resources management, governance and Tribunal activities of the Centre respectively.

e) Where possible and if it can serve the same purpose, the Personal Information described in sections 2.1 e) and 2.1 f) will be used in aggregate forms.

f) Access to, use and disclosure of Personal Information will be limited to the Centre's Employees, Board Members, Dispute Resolution Professionals, OSIC Professionals and Third Parties in accordance with the reasonable limits required to fulfill their duties and responsibilities with the Centre.

g) Personal information that is subject to a request shall be retained for as long as is necessary to allow the Individual to exhaust any recourse that he/she may have;

h) Any Personal Information collected by the Centre shall be managed in accordance with Section 6 herein, *Safeguards and Security*.

### 4.3 Retention

a) Personal Information shall be retained only as long as reasonably necessary and still relevant for the purposes for which it was collected.

b) As a general rule, retaining Sensitive Personal Information requires stronger or more compelling reasons and justifications than retaining other types of Personal Information.

c) Procedures for the retention, backups and archiving of Personal Information shall be in accordance with the Safeguard and Security standards stated in Section 6 herein and Appendix A of the *International Standard for the Protection of Privacy and Personal Information*, as published and amended from time to time by the Word Anti-Doping Agency.

## 5 – Accuracy of Information

a) The Centre will take reasonable steps to ensure that Personal Information is accurate, complete, and as up-to-date as is necessary for the identified purposes.

b) The Centre requires that each Individual be responsible to provide accurate Personal Information and to ensure it remains current by communicating any changes promptly to the Centre.

c) The Centre is not responsible for any loss of services or benefits resulting from Individuals who fail to advise the Centre in writing of any changes to their Personal Information on file.

## 6 – Safeguards and Security

### 6.1 General Provisions

a) The Centre has implemented safeguards to protect against loss, theft, unauthorized access, disclosure, copying, use or modification of Personal Information. These security safeguards vary according to the sensitivity of Personal Information; the more sensitive the information the higher the level of protection. The Centre commits to maintain those measures or equivalent ones as they may be modified from time to time.

b) The security methods employed by the Centre include, but are not limited to:

   i. Physical measures including, but not limited to, securing documents containing Personal Information in lockable filing cabinets and safes, controlling access to offices and filing cabinets to Employees only and shredding of paper files no longer in use;

   ii. Administrative measures including, but not limited to, appointing a Privacy Officer, limiting access to data on a need-to-know basis, providing confidentiality training and requiring the signature of confidentiality agreements before providing access to Personal Information; and

iii. Technological measures including, but not limited to, managing access to the Centre's office server, securing data transmission protocols, applying reasonable standards of data security to the Case Management Portal, permanently deleting emails after they have been downloaded as well as a disaster recovery plan.

## 6.2 Specific Areas of Safeguarding

a) Personal Information stored on the Centre's server and computers will be safeguarded as follows:

   i. Access to specific areas of the server is restricted through individual password-protected user accounts, based on personal profile of each Employee's responsibilities and needs; and

   ii. Backups are stored on password-protected devices and kept in a safe.

b) Any necessary transfer of Personal Information held by the Centre shall be conducted as follows:

   i. All servers used by the Centre, including the server hosting the Case Management Portal and OSIC Complaint Management Portal, are physically located in Canada, including any server redundancy equipment;

   ii. The Centre does not transfer Personal Information through cloud technologies and limits to the extent possible the transfer of Personal Information by electronic mail;

   iii. Email messages containing Personal Information shall be marked as being confidential and sent only to authorized recipients;

   iv. Where temporary copies, on any devices, are required for Employees to work remotely, duplicates are permanently deleted as soon as no longer needed.

c) Personal Information stored on the Case Management Portal and OSIC Complaint Management Portal shall be safeguarded as follows:

   i. Access to the Case Management Portal and OSIC Complaint Management Portal administration area is granted exclusively to Employees and to Third Parties responsible for technical support through password-protected user accounts;

   ii. Access to case-specific areas of the Case Management Portal and OSIC Complaint Management Portal is restricted to Employees, Dispute Resolution Professionals, OSIC Professionals, Parties and their Authorized Representatives who are concerned by this specific case, and Third Parties through password-protected user accounts;

   iii. Personalization of Case Management Portal and OSIC Complaint Management Portal passwords is governed by rules imposing robust password strength;

   iv. All files uploaded to the Case Management Portal and OSIC Complaint Management Portal are encrypted; and

   v. The entire case files on the Case Management Portal are permanently deleted on the 21st day following the case being declared closed by the Centre. Where a case

is subject to further appeals and at the request of Parties and their Authorized Representatives, the above period may be extended until such time as the subsequent proceedings are terminated. For clarity, this timeline shall not apply to case file and information contained on the OSIC Complaint Management Portal, which information shall be maintained indefinitely.

d) The Centre's Chief Executive Officer is the only person with access to Employee personnel files.

## 6.3 Privacy Education, Training and Agreements

a) All Employees, Board Members, Dispute Resolution Professionals and OSIC Professionals shall take part in an orientation session, which includes training on the Policy as well as clear directives related to the collection, use and disclosure of Personal Information, in the execution of their respective duties with the Centre.

b) All Employees, Board Members, Dispute Resolution Professionals and OSIC Professionals shall, prior to the commencement of their employment, term or mandate with the Centre, execute some form of agreement which binds them to the Centre's Policy as follows:

   i. All Employees shall sign an employment contract containing a confidentiality clause and are required to commit in writing, annually, to abide by the relevant provisions of the Centre's Workplace/Employment Policy and Procedures Handbook;

   ii. All Board Members upon appointment shall sign a confidentiality agreement which stipulates that they agree to respect the confidentiality of information that they may be privy to during the course of their duties, in accordance with the confidentiality policies of the Centre; and

   iii. All Dispute Resolution Professionals and OSIC Professionals shall, upon appointment by the Centre, sign a memorandum of agreement that refers to the Policy and the Centre's Mediators and Arbitrators Code of Conduct or other relevant OSIC policies and procedures (as applicable)

c) Where Personal Information is being disclosed to or used by a Third Party, the Centre shall ensure that such Third Parties adhere to the safeguard and security standards of the Centre through contractual means.

d) Parties and their Authorized Representatives are bound by the relevant provisions of the *Canadian Sport Dispute Resolution Code* which stipulate that they and any other persons attending the proceedings on their behalf shall not disclose any information or document obtained through their participation in the resolution process, unless required by law.

## 6.4 Destruction, Deletion or De-Identification

a) Personal information will be destroyed, deleted, permanently anonymized or, in the case of paper files, shredded, once it is no longer relevant or necessary for the purposes of the collection.

# 7 – Individual Access and Correction

## 7.1 Access and Corrections to Information

Subject to section 7.4,

a) It is the right of any Individual to access his or her Personal Information upon Request;

b) The Centre shall also provide, upon Request, an account of the use of the Individual's Personal Information, including disclosure to Third Parties;

c) The Individual is entitled to Request the correction of any demonstrable errors; and

d) Where necessary for the conduct of its operations or the maintenance of services and benefits to the Individual, the Centre shall transmit the amended Personal Information to Third Parties with authorized access.

## 7.2 Identification

a) Only Requests made in writing by Individuals having properly identified themselves or by Authorized Representatives having the proper authority on behalf of such Individual to obtain the requested Personal Information may be fulfilled.

b) Proper identification of the requestor shall include two government issued identification document (passport, driver's license, birth certificate, etc.), at least one of which must bear a photo of the requestor.

## 7.3 Time to Respond to Request

a) The Centre shall respond no later than 30 days from the date of receipt of a written Request by an Individual.

b) Under reasonable circumstances including, but not limited to, Requests of voluminous information, impracticable Requests, or Requests requiring a conversion of information, the Centre may require an extension of time beyond the 30-day time limit. In such cases, the requestor will be notified in writing before the expiration of the 30 days, of the reasons for extending the time limit and of their right to make a complaint to the Privacy Officer in respect of the extension.

## 7.4 Refusing a Request

a) The Centre may refuse a correction Request, with reasons, under certain limited instances including, but not limited to, where the Individual fails to provide sufficient proof that such information is incorrect. When it is impossible to amend a document, the correction shall be made by a note to file.

b) Despite a general right to access Personal Information upon Request, the Centre may refuse an access Request if the information is protected by solicitor-client privilege, litigation privilege or settlement privilege, or, in civil law, by the professional secrecy of lawyers and notaries;

c) The Centre may err on the side of caution and deny any such access Request in certain other situations such as, but not limited to:

   i. Fulfilling the access Request may cause harm to the Individual or to another Individual;

   ii. Fulfilling the access Request may compromise the administration, investigation or preparation for adjudication of a Complaint;

   iii. Fulfilling the access Request would reveal Personal Information of another Individual that is not severable without his or her consent, and is not needed to avoid harm to that other individual; or

   iv. Any reasonable doubt exists in the proper identification or authority of the requestor, whether the Individual or the person alleged to have authority to act on behalf of the Individual.

d) The Centre may, where reasonable and possible, allow access to Personal Information in a redacted form in order to avoid harm.

e) The Centre will be deemed to have refused an access Request if it fails to respond within the 30-day time limit.

# 8 – Challenging Compliance

## 8.1 Receipt of Inquiries and Complaints

a) All privacy inquiries, concerns and complaints are to be forwarded to the Privacy Officer upon receipt.

b) The Privacy Officer shall encourage, but not require, Individuals to submit their inquiries, concerns or complaints in writing.

c) An Individual may also file a written complaint with a Privacy Officer under applicable privacy legislation.

## 8.2 Handling of Inquiries and Complaints

a) When an Individual makes an inquiry or lodges a concern or a complaint regarding a possible confidentiality breach by:

   i. a Party, the Privacy Officer shall refer the Individual to the relevant provisions of the *Canadian Sport Dispute Resolution Code* on breaches of such code or to the relevant OSIC policies and procedures, as applicable;

   ii. a Dispute Resolution Professional or an OSIC Professional relating to a proceeding governed by the *Canadian Sport Dispute Resolution Code* or otherwise pursuant to an OSIC policy or procedure, the Privacy Officer shall refer the Individual to the Centre's *Complaints Process Policy*; and

   iii. an Employee, Board Member or Third Party, the Privacy Officer shall refer the Individual to the section 8.2 of the Policy and comply with this section.

b) Unless the Privacy Officer determines that there is sufficient cause to handle the inquiry, concern or complaint in another manner, the Centre will investigate all concerns and complaints.

c) The Privacy Officer will complete an initial review of any concerns or complaints within a reasonable period of time. In any event, the Privacy Officer will inform the Individual having lodged the concern or complaint of the progress of the review with an estimated date of completion.

d) If a concern or complaint is not resolved to the satisfaction of the Individual, the Centre will:

    i. record the substance of the unresolved concern or complaint with the relevant records about the Individual; and

    ii. where appropriate, transmit the existence of the unresolved concern or complaint to any Third Parties having access to the Personal Information in question.

## 8.3 Privacy Breaches

a) Privacy breaches include, but are not limited to, any inadvertent or intentional theft or loss of Personal Information, any unauthorized collection, use or disclosure of Personal Information, any unauthorized modification or destruction of Personal Information, or any non-compliance with this Policy.

b) In the event of any actual or suspected incidents of privacy breaches, the Privacy Officer shall report to either the Chairperson of the Board of Directors or the Chief Executive Officer of the Centre.

c) The Privacy Officer is obligated to ensure, minimally:

    i. Containment from further harm and unauthorized theft, loss, use, or disclosure;

    ii. Prompt notification of all affected, or possibly affected, Individuals;

    iii. Investigation of the breach, including a review of relevant systems and policies, and practices and procedures; and

    iv. Recommendations to, at his or her discretion, either the Chairperson of the Board of Directors or the Chief Executive Officer of the Centre for remediation, rectification and, where appropriate, disciplinary measures.

d) The Privacy Officer shall keep a record of all incidents and notifications with supporting reasons and inform the Individual of the outcome of the investigation regarding his or her concern or complaint.

## 8.4 Independent Audit

a) As deemed necessary, the Centre's Board of Directors, may initiate an independent audit of its own compliance with the Policy.

# Appendix A

The Centre collects Personal Information in respect of Individuals for the purposes set out below:

## From and about all Individuals:

- to organize events involving their participation;
- to refund admissible expenses incurred by Employees, Board Members or Third Parties, in the form of invoices, receipts and travel information;
- to respond to the Individuals' complaints or inquiries;
- to receive, process, administer, investigate, mediate and adjudicate Complaints related to the matter of the UCCMS, to publish decisions rendered pursuant to the UCCMS, and to maintain a registry of relevant information regarding Complaints and adjudication under the UCCMS;
- to assist the Individuals with administrative or technical support in the use of the Centre's systems and services;
- to collect the Individuals' opinions and comments in regard to the Centre's operations;
- to administer the physical security of the Centre's office, through the collection of Personal Information of visitors and clients in the form of images captured on the security video surveillance system;
- such other collections and uses of Personal Information from such persons and for such purposes for which the Centre may obtain consent from time to time; and
- as otherwise required or permitted by law.

## From Individuals other than Employees:

- as part of the Individuals' requests for the Centre's dispute resolution services or dispute prevention services;
- as part of the Individuals' applications to participate in one of the Centre's programs;
- to advise Individuals about new programs and services that may be of interest to them or to their organizations;
- to monitor the use of the Case Management Portal and OSIC Complaint Management Portal and detect possible fraudulent attempted use; and
- for the purposes of statistical reporting and clients' sport profiles.

## From Employees:

- for the purpose of recruitment for positions at the Centre;
- for the purpose of the administration of the Centre's policies and procedures regarding the training, retention and evaluation of Employees;
- for the purposes of coaching, mentoring and professional development;
- for the purposes of managing productivity, including making accommodations and allowances;
- from Third Party providers of benefits, pension arrangements and insurance and other related Employee services, for the purpose of providing compensation and such services and fulfilling taxation requirements in respect of same;

- to comply with other requirements imposed by law including, but not limited to, collecting Personal Information as required by applicable workplace insurance and safety legislation and occupational health and safety legislation; and
- for the purpose of assisting in the administration of Workers' Compensation program after a work-related illness or injury.