CCES Privacy Policy

Version Number: Final Version 1 approved by Jeremy Luke
Effective Date: January 1, 2025

Table of Contents

Overview

This document sets out the privacy policy for the Canadian Centre for Ethics in Sport (the "Privacy Policy"). This Privacy Policy is set out in four parts:

Part 1	Outlines privacy policies applicable to the Canadian Centre for Ethics in Sport (CCES) as an organization.
Part 2	Outlines privacy policies applicable specifically to the CCES's Canadian Anti-Doping Program.
Part 3	Outlines privacy policies applicable specifically to the CCES's Canadian Safe Sport Program.
Part 4	Outlines related to policies to the CCES's Privacy Policy.

PART I: CCES PRIVACY POLICY

1.1 Introduction

The Canadian Centre for Ethics in Sport is an organization that functions as a regulator. This privacy policy ("Privacy Policy") sets out the overarching privacy policies that apply to the organization as a whole, and it separates out the privacy policies that apply specifically to the CCES's role in the Canadian Anti-Doping Program (the "**CADP**"), and specifically to the Canadian Safe Sport Program (the "**CSSP**").

This Privacy Policy is developed in part in conjunction with the World Anti-Doping Agency's ("**WADA**") International Standard for the Protection of Privacy and Personal Information ("**ISPPPI**") and it reflects the policies and principles set out in applicable legislation and regulations. The intent of the CCES Privacy Policy is four-fold:

i. To be fully compliant with WADA's privacy requirements regarding the CADP;
ii. To be fully compliant with all applicable Canadian privacy legislation and regulations;
iii. To fully comply with the CCES's contractual obligations regarding privacy and data protection measures entered into with third parties; and,
iv. To fulfill the CCES's responsibilities to those from whom it collects and retains personal information.

The CCES is also committed to taking reasonable steps to ensure that third-party organizations that receive, collect, retain, safeguard, use, and destroy personal information on behalf of the CCES, have appropriate privacy and data management systems in place.

Refer to the WADA ISPPPI.

1.2 Definitions

CCES Defined Terms:

CCES Employee, Contractor or Volunteer: any individual acting in a role on behalf of the CCES that involves Processing Personal Information**.**

Partner: a Third-Party organization and/or client retaining the CCES to provide anti-doping services.

Personal Information: means any information provided to or collected by the CCES about an identifiable individual**.** For clarity, Personal Information excludes reports, work product, and other information prepared by the CCES.

Service Agreement: any kind of arrangement or contract with any individual or organization who provides the CCES with any kind of service that involves the processing of Personal Information under the control of the CCES or anti-doping service that involves the processing of Personal Anti-Doping Information under the control of the CCES.

Sub-processor: any service provider who provides the CCES with any kind of service that involves the Processing of Personal Information with respect to which the CCES is acting as a Data Processor.

In addition, throughout the Privacy Policy additional terms have the meanings specifically attached to them as indicated in the text.

All capitalized terms used in Part I but not otherwise defined shall have the same meaning as set out in the WADA ISPPPI.

Defined Terms from the WADA ISPPPI that Apply to the CADP:

Personal Anti-Doping Information: Information, including without limitation Sensitive Personal Information, relating to an identified or identifiable Participant or other Person whose information is Processed solely in the context of an Anti-Doping Organization's Anti-Doping Activities. [Comment regarding Personal Anti-Doping Information – It is understood that Personal Anti-Doping Information includes, but is not limited to, information relating to an Athlete's name, date of birth, contact details and sporting affiliations, whereabouts, designated TUEs (if any), anti-doping test results, and Results Management (including disciplinary hearings, appeals and sanctions). Personal Anti-Doping Information also includes personal details and contact information relating to other Persons, such as medical professionals and other Persons working with, treating or assisting an Athlete in the context of Anti-Doping Activities. Such information remains Personal Anti-Doping Information and is regulated by this International Standard for the entire duration of its Processing, irrespective of whether the relevant individual remains involved in organized sport.] For further clarity, Personal Anti-Doping Information excludes reports, work product, and other information prepared by the CCES.

Processing (and its cognates, Process and Processed): Collecting, accessing, retaining, storing, disclosing, transferring, transmitting, amending, deleting or otherwise making use of Personal Anti-Doping Information.

Security Breach: A breach of security resulting in the loss, theft, damage or unauthorized and/or unlawful Processing of Personal Anti-Doping Information whether in electronic or hard-copy or other form, or interference with an information system, that compromises the privacy, security, confidentiality, availability or integrity of Personal Anti-Doping Information.

Sensitive Personal Information: Personal Information relating to a Participant's racial or ethnic origin, commission of offences (criminal or otherwise), health (including information derived from analyzing an Athlete's Samples or Specimens), and biometric and genetic information.

Third Party: Any Person other than the Person to whom the relevant Personal Anti-Doping Information relates, Anti-Doping Organizations, and Third-Party Agents.

Third-Party Agent: Any Person that Processes Personal Anti-Doping Information on behalf of, as delegated by, or as otherwise engaged by an Anti-Doping Organization in the context of ISPPPI the Anti-Doping Organization's own Anti-Doping Activities including, without limitation, a Delegated Third Party and any subcontractors.

Defined Terms from the WADA International Standard for Testing and Investigations (ISTI):

Testing Authority: The Anti-Doping Organization authorizes Testing on Athletes it has authority over. It may authorize a Delegated Third Party to conduct Testing pursuant to the authority of and in accordance with the rules of the Anti-Doping Organization. Such authorization shall be documented. The Anti-Doping Organization authorizing Testing remains the Testing Authority

and ultimately responsible under the Code to ensure the Delegated Third Party conducting the Testing does so in compliance with the requirements of the International Standard for Testing and Investigations.

1.3 Background Information

The CCES performs a wide range of anti-doping services including being Canada's national anti-doping agency. The CCES is responsible for implementing the Canadian Anti-Doping Program ("**CADP**") and offering related services for Partners and clients (such as international sports federations and major games). This Privacy Policy relates in part to the implementation of the CADP and providing other anti-doping services.

The CCES is also responsible for independently administering the Universal Code of Conduct to Prevent and Address Maltreatment in Sport (the "**UCCMS**") through the Canadian Safe Sport Program (**"CSSP"**) at the national level for federally funded Canadian sport organizations. This Privacy Policy also relates in part to the implementation of the CSSP.

The CCES is committed to handling Personal Information under the CSSP and CADP in compliance with all applicable privacy legislation and regulations, all contractual rights and obligations regarding privacy and data protection measures entered into with third parties (including consents to the collection, use or disclosure of personal information); and the CCES's responsibilities to those from whom it collects and retains Personal Information.

Moreover, the CCES is committed to handling CADP Personal Anti-Doping Information in compliance with WADA ISPPI. The CCES Processes and manages different types of Personal Anti-Doping Information, sometimes as an entity controlling the data (also referred to as a "Data Controller"), and in other situations, on behalf of Partners and clients (also referred to as a "Data Processor"). Part II of the Privacy Policy discusses this in more detail.

1.4 Objective and Scope

This Privacy Policy establishes appropriate policies, practices, procedures and systems for handling of Personal Information to help ensure that the CCES complies with the requirements of Canadian law, and in addition for the CADP, the requirements contained in the WADA ISPPPI and the requirements contained in contracts entered into between the CCES and its various Partners (together the "CCES Privacy Obligations"). In both cases, the CCES wishes to ensure that it has in place all proper safeguards to protect Personal Information in its custody or control. This Privacy Policy, or parts thereof:

- Applies to any CCES employee, contractor or volunteer responsible for Processing Personal Information.
- Explains how such CCES employees, contractors or volunteers are required to handle Personal Information to help ensure that the CCES Privacy Obligations are satisfied.
- Controls the management and destruction of Personal Information, defines the roles and responsibilities of the CCES employees, contractors and volunteers throughout the life cycle of the information and provides a process for dealing with complaints regarding the processing of Personal Information.

- Applies to Personal Information in the CCES's custody or control, including Personal Information that has been transferred by the CCES to a service provider for Processing on behalf of the CCES.
- Applies to Personal Information processed on behalf of Partners, even if the CCES has transferred such information to a Sub-processor for processing.
- Ensures that, for the CADP, the CCES is only collecting relevant and proportionate Personal Anti-Doping Information for legitimate anti-doping purposes pursuant to the CADP and the World Anti-Doping Code.
- Ensures that, for the CSSP and the UCCMS, the CCES is only collecting relevant and proportionate Personal Information for the legitimate safe sport purposes pursuant to the CSSP and the UCCMS.

All the CCES employees, contractors and volunteers who process Personal Information are required to read and be familiar with relevant aspects of this Privacy Policy or some specific work instruction to cover off their scope of Processing Personal Information and/or related documents. The CCES employees, contractors and volunteers will handle Personal Information in accordance with this Privacy Policy. Employees shall be comfortable guiding volunteers, Board of Directors and Sub-processors on Personal Information requirements that relate to their agreements with the CCES. Questions can be directed to the Privacy Officer who will rely on appropriate expertise/experience to guide others along.

1.5 Privacy Officer

Privacy Officer Role: The CCES shall appoint a person responsible for the protection of Personal Information (the "**Privacy Officer**"). The Privacy Officer's role includes, but is not limited to, ensuring that:

1. The CCES implements and complies with the CCES Privacy Obligations;
2. The CCES's Privacy Policy complies with applicable laws, regulations, and governing policies; and
3. The CCES properly investigates, responds to, and reports privacy complaints and breaches.

The Privacy Officer's specific responsibilities are enumerated in more detail below.

The Privacy Officer shall be able to delegate all or part of its function in writing to other CCES employee(s). CCES employees shall transfer any inquiry or complaint relating to the management of Personal Information to the Privacy Officer as per section 1.10 of this Privacy Policy.

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

All inquiries or complaints relating to the management of Personal Information shall be forwarded to the Privacy Officer. The Privacy Officer's contact information is detailed below.

Privacy Officer Appointment: The CCES shall appoint a Privacy Officer who possesses the necessary qualifications, expertise, and experience in privacy and data protection. The Privacy Officer shall report directly to the CEO.

Responsibilities of the Privacy Officer: The Privacy Officer shall have the following responsibilities:

1. Compliance Oversight:
    a. Ensure the CCES's CADP policies are fully compliant with WADA's privacy requirements and all applicable Canadian privacy legislation.
    b. Monitor changes in privacy laws and regulations and update the Privacy Policy accordingly.
2. Policy Development and Implementation:
    a. Develop, implement, and maintain privacy policies, procedures, and guidelines in alignment with the Privacy Policy.
    b. Ensure that all privacy policies are effectively communicated to and understood by all relevant personnel.
3. Data Protection Impact Assessments
    a. Conduct Data Protection Impact Assessments ("DPIAs") for new projects, systems or processes that involve the processing of Personal Information.
    b. Identify and mitigate privacy risks associated with data processing activities.
4. Training and Awareness:
    a. Develop and deliver privacy training programs for employees, contractors, and other relevant stakeholders.
    b. Promote a culture of privacy awareness and compliance within the organization.
5. Incident Management and Breach Response
    a. Establish and maintain procedures for identifying, reporting, and managing data breaches and security incidents.
    b. Lead the investigation and response to data breaches, including notification to affected individuals and regulatory authorities as required.
6. Inquiries and Complaints Handling
    a. Serve as the primary point of contact for privacy-related inquiries and complaints from individuals, regulators, and other stakeholders.
    b. Ensure that inquiries and complaints are addressed promptly and in accordance with established procedures.
7. Record-Keeping and Organization
    a. Maintain accurate records of data processing activities, DPIAs, data breaches, and other relevant documentation.
    b. Ensure that records are kept in compliance with legal and regulatory requirements.

Authority of the Privacy Officer: The Privacy Officer shall have the authority to:

8. Access to Information
    a. Access all necessary information and resources required to perform their duties effectively.
    b. Conduct audits and assessments of data processing activities to ensure compliance with the Privacy Policy.
9. Decision-Making

   a. Make decisions regarding the implementation of privacy controls and measures to mitigate identified risks.
   b. Approve or reject data processing activities that do not comply with the Privacy Policy or pose significant privacy risks.
10. Reporting and Accountability
   a. Report regularly to the Executive Management Team on the status of privacy compliance, risks, and incidents.
   b. Escalate significant privacy issues to senior management and recommend corrective action.

Support and Resources: The CCES shall provide the Privacy Officer with the necessary support and resources to fulfill their responsibilities effectively. This includes access to training, legal advice, and technical tools required for privacy management.

Privacy Officer's Contact Information: The Privacy Officer's contact information will be published on the CCES's website at all times. Upon request, CCES employees will provide individuals with the contact information of the Privacy Officer.

The Privacy Officer may be contacted by email at: privacy@cces.ca.

The Overview of the Privacy Policy shall be made publicly available through the CCES's website(s) and upon request.

The CCES shall make accessible, through the Privacy 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 CCES's records; and
iii. Where Personal Information is shared with third parties, a justification for giving access to those third parties.

1.6 Challenging Compliance

Receipt of Inquiries and Complaints: All written privacy inquiries, concerns and complaints are to be forwarded to the Privacy Officer upon receipt.

Handling of Inquiries and Complaints: 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 CADP, CSSP, UCCMS, and this Policy; or

ii) A Contractor - the Privacy Officer shall refer the Individual to this Privacy Policy.

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

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.

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

a) record the substance of the unresolved concern or complaint with the relevant records about the Individual; and
b) where appropriate, transmit the existence of the unresolved concern or complaint to any third parties having access to the Personal Information in question.

Privacy Breaches: 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.

The Privacy Officer is obligated to ensure, minimally:

a) Containment from further harm and unauthorized theft, loss, use, or disclosure;
b) Prompt notification of all affected, or possibly affected, Individuals;
c) Investigation of the breach, including a review of relevant systems and policies, and practices and procedures; and
d) Recommendations to the Chief Executive Officer of the CCES for remediation, rectification and, where appropriate, disciplinary measures.

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.

Independent Audit: As deemed necessary, the CCES's Board of Directors, may initiate an independent audit of its own compliance with the Policy.

1.7 Accuracy and Access to Personal Information

Data Accuracy: When acting in a capacity of Data Controller, the CCES shall ensure Personal Information is accurate, complete, and up to date as is necessary for the purposes for which the information is to be used. Where Personal Information is demonstrated to be inaccurate, incomplete, or not up to date, CCES shall correct and update Personal Information as necessary and upon request. The CCES will rectify or amend Personal Information under its custody or control as soon as practically possible.

Receiving Access Requests: Individuals interacting with CCES will be informed about their access rights contained in the Privacy Policy. CCES employees who receive a request by an individual for information about, or access to, their Personal Information held by the CCES shall redirect and transfer this request by email to the Privacy Officer who will manage such requests in accordance with this Section 1.5 and 1.10 of the Privacy Policy.

Managing Access Requests: The Privacy Officer shall only process individual's access requests made in writing and manage such requests in accordance with the process detailed in this section. For access requests pertaining to the CADP, such requests will also be required to be in conjunction with the ISPPPI Section 11.1-3 which has detailed requirements:

- **As Data Controller**: Upon receiving an access request as a Data Controller, the Privacy Officer shall confirm receipt of the request to the individual within a reasonable timeframe and provide such individual with information about how it intends to process the request, including the method for verifying the individual's identity, if necessary. The communication confirming receipt shall request:
    i) any missing information necessary to identify the individual making the request (if necessary); and
    ii) any clarifications to enable the CCES to locate the information being requested and adequately respond to the individual request (e.g., details on the information requested).

- **As Data Processor:** Upon receiving an access request from an individual that the CCES interacts with in the capacity of a Data Processor, the Privacy Officer shall not answer such request, shall transfer the request to the relevant Partner, and inform the individual who has made the request that the request has been transferred to the relevant Partner who is the Data Controller**.**

- **Answering Access Requests:** The CCES shall transfer to a Partner or process and respond to access requests within 30 days. Where applicable, the Privacy Officer shall review the WADA ISPPPI Section 11 (1-3) requirements/considerations and shall provide the CCES's answer in writing and consider whether the request may be transferred to a Partner or accepted or denied, in whole or in part, in circumstances detailed in the WADA ISPPPI, including situations where disclosing the information to the individual making the request would reveal:

    i) Personal Information about a third person, which may seriously harm that person;
    ii) information protected by solicitor-client privilege or professional secrecy of lawyers; and,
    iii) information which would likely affect judicial proceedings in which either the CCES or the individual making the request has an interest.

1.8 Outsourcing the Processing of Personal Information

Outsourcing: In appropriate circumstances, the CCES may transfer Personal Information to service providers or, when processing Personal Information on behalf of a Partner, to Sub-processors. The CCES shall use contractual means to appropriately protect Personal Information while it is being processed by service providers/Sub-processors in accordance with this section. All Service Agreements involving the processing of Personal Information by a Third Party shall be approved by the CCES's Privacy Officer.

Contract Minimum Requirements / Use of template Data Processing Addendum (DPA). The Service Agreement between the CCES and a service provider/Sub-processor shall be in writing and provide at a minimum: (i) mandatory compliance with applicable privacy legislation and a description of the measures taken by the service provider/Sub-processor to ensure the

confidentiality of the Personal Information (e.g., a description of the security safeguards); (ii) an obligation for the service provider/Sub-processor to only use the Personal Information for the purposes of rendering the services to the CCES, and to not keep such information after the expiration or termination of the contract and provide the CCES, upon request, a written confirmation of compliance with this requirement by an officer of the service provider/Sub-processor; and (iii) an obligation for the service provider/Sub-processor to notify the CCES's Privacy Officer without delay of any actual or attempted Security Breach and to allow the Privacy Officer to conduct any verification relating to information security requirements. When applicable, and whenever possible, the CCES shall enter into the CCES Controller DPA with service providers/Sub-processors.

Sub-processing Requirements: Before transferring Personal Information to a Sub-processor, the CCES shall ensure it is authorized to do so under its contract with the relevant Partner(s). Even if sub-processing is authorized, the contract with the relevant Partner may require that the CCES includes additional protections (in addition to the contract minimum requirements discussed above) in its contracts with Sub-processors.

Ongoing Monitoring: The CCES shall grant itself various oversight and monitoring rights through any contractual arrangement with a service provider/Sub-processor, such as the right to request the service provider to provide reports, information and certifications, and rights to conduct audits or investigations of the service provider. The CCES employee responsible for developing the Service Agreement shall regularly use those rights to assess service provider/Sub-processor's compliance and immediately report to the Privacy Officer any incident or event that has affected, or is likely to affect, the security, confidentiality, integrity or availability of any Personal Information.

Termination of Outsourcing Arrangement: At the end of a Service Agreement, the CCES employee overseeing that contract shall ensure that the service provider returns all the Personal Information to the CCES, securely deletes/destroys all records of the CCES data in its possession or control and deliver a written confirmation of compliance to the CCES. The employee shall further take steps to manage information security risks when a Service Agreement ends including, for example, cancelling a service provider's credentials to remotely access the CCES's systems and Personal Information.

1.9 Information Security and Security Breaches

Information Security: The CCES will use appropriate security measures to safeguard Personal Information in its custody or control. All the CCES employees, contractors and volunteers will exercise caution and care when handling Personal Information, and shall use appropriate security measures (physical, organizational, and technological) to safeguard Personal Information in accordance with this Privacy Policy and other relevant CCES policies and procedures. More specifically, the CCES employees, contractors and volunteers' access to Personal Information is limited to the extent required to perform their assigned duties, and with respect to service providers, Sub-processors, advisors or other Third Parties with whom the CCES may share such information, access is limited to those who have a genuine need to access Personal Information in the course of their mandate for the CCES and only to the extent necessary to fulfill their mandate.

Security Breaches: A Security Breach occurs when there is any loss, destruction or alteration of Personal Information, or any unauthorized access or disclosure of Personal Information. For example:

- **Accidental disclosure:** Personal Information is disclosed to an unintended recipient by accident. For example: (i) an email or letter containing Personal Information is sent to the wrong address due to mechanical or human error; (ii) Personal Information is made available online by CCES through a technical glitch.
- **Loss:** Personal Information goes missing. For example, a CCES employee's laptop, mobile device or backpack containing Personal Information is lost.
- **Unauthorized Access or Disclosure:** Personal Information is accessed by or disclosed to an unauthorized person, or in an unauthorized manner, or for an unauthorized purpose, including in contravention of any of the CCES's applicable policies, procedures or Partner contracts.

Reporting Security Breaches within the CCES: The CCES employees, contractors and volunteers shall remain vigilant for breaches of security safeguards and will immediately report any actual or reasonably suspected breach to the Privacy Officer. Immediate reporting of an actual or suspected Security Breach will allow the Privacy Officer to promptly investigate and respond to the breach, to help protect the CCES and all affected individuals and other organizations. The sooner the CCES can act regarding a Security Breach, the better it will be able to effectively contain the breach and avoid and mitigate resulting harm.

Confirming the Security Breach: The Privacy Officer shall investigate any report of a Security Breach brought to its attention; a high-level assessment of the situation shall immediately be carried out by the Privacy Officer who shall determine if the suspected incident is a confirmed Security Breach. If the Security Breach is confirmed, the following steps shall be undertaken:

- **Step 1: Creation of a Breach Management Team.** The Privacy Officer shall appoint members of a breach management team, considering for such appointments the CCES employees who may have any useful or necessary knowledge and/or expertise. At the same time, the CCES General Counsel and the Executive Director, Corporate Services will take any actions to advise the CCES insurers.

- **Step 2: Containment of the Breach.** This breach management team shall ensure the Security Breach is immediately contained by (i) closing the breach, including if applicable, by putting an end to the unauthorized practice, recovering all relevant records, shutting down the system or access to the system that relates to the breach, revoking or changing computer access codes, correcting vulnerabilities in physical or electronic security, or undertaking any other corrective action as appropriate; and (ii) protecting the investigation by protecting and preserving all evidence that could be valuable in determining the cause of the breach, including if applicable, by cloning electronic devices, preserving emails, and sending a litigation hold/document preservation notice to relevant Employees.

- **Step 3: Investigation**. The breach management team shall coordinate the investigation and confirm the risks posed by the Security Breach, define an action plan to investigate

such breach, coordinate the implementation of the action plan, and oversee the completion of an investigation report. The breach management team shall also oversee the Security Breach resolution process, ensure that all relevant risks are properly addressed, review the investigation report, and ensure the Security Breach is thoroughly investigated, documented, and properly resolved.

- **Step 4: Identify the Parties to Notify.** The Privacy Officer shall determine whether there is a legal obligation (or if it is otherwise appropriate) to send a declaration to privacy regulators and a notice to affected individuals, by considering whether the Security Breach presents a real risk of significant harm (or similar criterion under applicable law) to affected individuals, taking into account the sensitivity of the information concerned, the anticipated consequences of its use and the likelihood that such information will be used for injurious purposes. The Privacy Officer shall also determine whether there is a legal or contractual obligation to send a notice to external parties, including (i) to Partners (if it sustains a Security Breach affecting Personal Information accessed by the CCES acting as a Data Processor), service providers or Sub-processors, as the case may be (if required by contract); (ii) law enforcement (if theft or other crime is suspected); (iii) insurers or others (if required by contract or if the breach may be insurable); (iv) professional or other regulatory bodies (if applicable); and (v) the Privacy Commissioner, if the CCES determines necessary.

- **Step 5: Document the Reporting Decision.** The Privacy Officer shall document its notification decisions, as outlined in Step 4 above. In doing so, the Privacy Officer shall outline its decision for reaching a conclusion on whether to notify either an affected individual or to report the data breach to a third party, law enforcement, insurers or others, professional or other regulatory bodies, and the Privacy Commissioner.

1.10 Regulators, Law Enforcement/Government and Legal Process

Regulators: CCES employees who receive correspondence or communications from a regulator which relates to the management of Personal Information shall immediately report the matter to the Privacy Officer for appropriate response on behalf of the CCES. The Privacy Officer is the single point of contact for all correspondence and communications with the regulator. The Privacy Officer will consult with and involve other CCES employees as appropriate in accordance with applicable CCES policies and guidelines. CCES employees are not to respond to correspondence or communications from a regulator unless specifically directed by the Privacy Officer.

Law Enforcement, Government and Legal Process: CCES employees who receive correspondence or communications from law enforcement or a government agency requesting access to Personal Information, or a subpoena or similar judicial request for access to Personal Information, shall immediately report the request to the Privacy Officer. The Privacy Officer is responsible for responding to those kinds of requests. CCES employees are not to respond to correspondence or communications from law enforcement or a government agency regarding a request to access Personal Information unless specifically directed by the Privacy Officer.

Inquiries or Complaints to the CCES

Individuals who believe there has been a breach of the Privacy Policy, or the ISPPPI, as applicable, are advised to send a confidential letter (by mail or password-protected email attachment), with details of their concern or complaint, to the Privacy Officer at the following addresses:

Email address: privacy@cces.ca
Toll-free number: 1.800.672.7775
By mail: 201-2723 Lancaster Rd
Ottawa, ON K0B 0B1

In addition, CCES employees who receive an inquiry or a complaint related to the handling of Personal Information from an individual shall promptly report the complaint and the individual's name and contact information (if available) to the Privacy Officer. CCES employees are not to respond to correspondence or communications from an individual unless specifically directed by the Privacy Officer.

Support and Enforcement

Support and Advice: A CCES employee, contractor or volunteer uncertain about the application of this Privacy Policy—and/or ISPPPI if they are dealing with the CADP—or that has a concern pertaining to a practice that may go against this Privacy Policy, shall direct all such inquiries to the Privacy Officer.

Enforcement: All CCES employees dealing with the CADP are required to comply with the WADA ISPPPI in addition to this Privacy Policy. Any CCES employee who violates this Privacy Policy, or ISPPPI if they are dealing with the CADP, may be subject to disciplinary action, up to and including termination.

1.11 Changes to this Privacy Policy

This Privacy Policy shall be reviewed and updated on a regular basis to ensure its continued relevance and effectiveness. These additions aim to provide a clear, structured approach to managing changes, ensuring stakeholder involvement, and maintaining compliance with evolving privacy laws, regulations, and policies of other organizations, like WADA. This Privacy Policy, as revised from time to time and reviewed regularly, may be found on the CCES network.

Stakeholder Involvement: The review and update process shall involve key stakeholders, including but not limited to:

- The Privacy Officer;
- The applicable legal and compliance teams;
- The information security team;
- Relevant department heads; and
- External privacy experts (if necessary).

Change Management Process: The following steps outline the change management process for updating the Privacy Policy:

1. **Identification of Changes**: Changes may be identified through various sources, including legislative updates, regulatory guidance, internal audits, risk assessments, and feedback from stakeholders.

2. **Impact Assessment:** An impact assessment shall be conducted to evaluate the potential effects of proposed changes on the organization's privacy practices and compliance obligations.
3. **Drafting Amendments**: The Privacy Officer, in collaboration with relevant stakeholders, shall draft the proposed amendments to the Privacy Policy. The draft shall include a rationale for the changes and any necessary supporting documentation.
4. **Review and Approval**: The draft amendments shall be reviewed by the CEO to ensure alignment with applicable laws and regulations. The final draft shall be submitted to CEO for approval.
5. **Communication and Training**: Once approved, the updated Privacy Policy shall be communicated to all relevant personnel. Training sessions shall be conducted to ensure understanding and compliance with the new provisions.
6. **Documentation and Record-Keeping:** All changes to the Privacy Policy shall be documented, including the rationale for the changes, the impact assessment, and the approval process. These records shall be maintained for audit and compliance purposes.

Emergency Updates: In the event of significant legal or regulatory changes that require immediate action, the Privacy Officer is authorized to implement temporary amendments to the Privacy Policy. These emergency updates shall be reviewed and ratified by the CEO at the earliest opportunity.

Version Control: Each version of the Privacy Policy shall be clearly numbered and dated. A version history log shall be maintained to track all changes, including the date of implementation and a summary of the amendments.

Continuous Improvement: The CCES is committed to continuous improvement of its privacy practices. Feedback from audits, risk assessments, and stakeholder input shall be used to identify areas for enhancement and inform future updates to the Privacy Policy.

Other Related CCES Policies, Procedures and Guidelines

Please also consider the following CCES policies and procedures in addition to the schedules:

- WADA ISPPPI
- Retention Schedules (WADA ISPPPI Annex A, Quality File Index, Corporate Operations)

This Privacy Policy was last updated on January 1, 2025

PART II: CADP SPECIFIC PRIVACY POLICY

2.1 Jurisdiction and Application

The CCES is responsible for administering the Canadian Anti-Doping Program (CADP). In doing so, the CCES ensures that the Personal Anti-Doping Information that it processes in connection with its anti-doping activities is protected in accordance with applicable data protection and privacy laws, principles and standards.

The CCES also complies with the provisions of the WADA ISPPPI as incorporated into the CADP.

This Policy sets out in general terms how Personal Anti-Doping Information for anti-doping purposes will be processed by the CCES in the course of administrating and implementing the CADP.

2.2 CADP Specific Definitions

Data Controller: the situation where the CCES is processing and managing Personal Information on its own behalf, further detailed in its Privacy Policy.

Data Processor: the situation where the CCES is acting in a service provider capacity, processing and managing Personal Information on behalf of a Partner or client (e.g., international sport federations and major games).

2.3 Types of Personal Anti-Doping Information for anti-doping

Personal Anti-Doping Information for anti-doping purposes includes, but is not limited to, information relating to an individual, as follows:

- identity (i.e., name, nationality, date of birth, gender, event, level of competition, membership affiliations, the names and details of other persons, such as medical professionals, working with, treating or assisting the individual in a sport and anti-doping context);
- Whereabouts Filings;
- Medical Exemptions, including Therapeutic Use Exemptions (TUEs), and Medical Reviews;
- Doping Controls (including Test Distribution Planning, Sample collection and handling, anti-doping test results, Laboratory analysis, results management, hearings, sanctions and appeals).

Personal Anti-Doping Information about an individual could also include Sensitive Personal Information, in particular this includes racial, ethnic, genetic, medical or biological information (including information derived from analysing Samples or Specimens) and commission of offences.

2.4 Collection Entity

Personal Anti-Doping Information of all sorts will be collected by the CCES and by any other organization or anti-doping organization to whom the CCES has delegated proper authority to

conduct Testing and Sample Collection in accordance with the CADP or which otherwise has competent authority to conduct Testing and Sample Collection on the individual.

2.5 Purposes for which your Personal Anti-Doping Information may be processed

The CCES and its third-party agents shall only process the collected Personal Anti-Doping Information where necessary and appropriate to conduct their anti-doping activities under the CADP and related WADA International Standards or where otherwise required by applicable law and where there is no conflict with applicable privacy and data protection laws. This includes, but is not limited to, processing Personal Anti-Doping Information:

- to determine eligibility for a TUE;
- to conduct Testing, including Target Testing, and to record the results from such Testing;
- to conduct investigations to determine potential breaches of the CADP;
- to carry out results management under the CADP, including associated disciplinary and hearings, appeals and adjudications, and to publish outcomes.

2.6 Disclosures

Personal Anti-Doping Information may be disclosed by the CCES to third party agents, including authorized service providers, in connection with the fulfilment of the CCES's anti-doping activities as specified in the CADP.

Personal Anti-Doping Information shall not be disclosed to other Anti-Doping Organizations except where such disclosures are necessary to allow the Anti-Doping Organizations receiving the Personal Anti-Doping Information to conduct anti-doping activities under the CADP or under the World Anti-Doping Code (Code) and in accordance with all applicable privacy and data protection laws.

Personal Anti-Doping Information shall not be disclosed to third parties other than as set out above, except where such disclosures:

- are required by law;
- take place on the basis of informed, express and written consent; or
- are necessary to assist law enforcement or governmental authorities in the detection, investigation or prosecution of a criminal offence or breach of the CADP, provided that the Personal Anti-Doping Information requested is directly relevant to the offence or breach in question and cannot otherwise be obtained by the authorities.

2.7 International Transfers

Personal Anti-Doping Information may be made available by the CCES to third persons or parties, including authorized service providers, WADA and Anti-Doping Organizations, some of which may be located outside of Canada.

Cross-border transfers: Before transferring Personal Anti-Doping Information outside of Canada, the CCES will:

- If it is acting as a Data Processor, ensure that such transfer is not prohibited under its contract with a Partner.

- If it is acting as a Data Controller, ensure that the concerned individuals have been informed that their Personal Anti-Doping Information may be transferred outside of Canada.
- In all cases, ensure that the technical security measures used to transfer the Personal Anti-Doping Information will be appropriate to the level of sensitivity of the information, in accordance with the CCES Information Security Procedure and WADA ISPPPI.

2.8 Rights with Respect to Personal Anti-Doping Information

Right of access to Personal Anti-Doping Information: Individuals have the right to seek information from the CCES about Personal Anti-Doping Information relating to them (the categories of information, the purpose for which it is collected and the third parties or categories of third parties to which it is transferred), to obtain confirmation whether or not the Personal Anti-Doping Information is being processed and to receive a copy of the relevant Personal Anti-Doping Information in a readily intelligible format within a reasonable timeframe (one month from the date of the request), unless to do so in a particular case plainly conflicts with the CCES's ability to plan or conduct Testing under the CADP (including Target Testing) or to investigate and establish anti-doping rule violations.

The CCES may not respond to requests seeking access to Personal Anti-Doping Information if the requests are excessive in terms of their scope or frequency or if they impose a disproportionate burden on the CCES in terms of cost or effort given the nature of the Personal Anti-Doping Information in question. If the CCES refuses to allow access to Personal Anti-Doping Information, it shall inform the relevant individuals and explain in writing the grounds for refusing the request as soon as practicable.

Right to amend Personal Anti-Doping Information: Personal Anti-Doping Information processed by the CCES shall be accurate, complete and kept up to date. Where the CCES affirmatively knows that the Personal Anti-Doping Information that it is processing is inaccurate or incomplete, the CCES shall, as appropriate, rectify, amend, complete, update or delete the relevant Personal Anti-Doping Information as soon as possible. Where appropriate, if the Personal Anti-Doping Information in question has been disclosed to a third party that is known or believed to continue to process the Personal Anti-Doping Information, the third party shall be informed of the change(s) as soon as possible.

Right to object to the processing of Personal Anti-Doping Information: Individuals have the right to object to the processing of their Personal Anti-Doping Information, although, in such event, it may still be necessary for the CCES and/or third parties to continue to process (including retain) certain of this Personal Anti-Doping Information in order to fulfil obligations and responsibilities arising under the CADP or applicable laws.

Objecting to disclose Personal Anti-Doping Information or objecting to the processing of Personal Anti-Doping Information may be construed as a refusal to participate and may result in an anti-doping rule violation. A refusal to permit the CCES to process properly collected Personal Anti-Doping Information may result in the individual thereby becoming non-compliant with the CADP, with all associated consequences

Right to initiate a complaint: Individuals are entitled to initiate a complaint where there is a reasonable good faith belief that the CCES is not complying with the CADP, a WADA International Standard or with any applicable law relating to privacy protection. The complaint shall be made to the CCES.

Complaints should be submitted to the CCES at privacy@cces.ca.

2.9 Processing Personal Anti-Doping Information

Processing Personal Anti-Doping Information as Data Controller

This section includes the fundamental rules for the CCES's processing of Personal Anti-Doping Information about individuals when the CCES is acting in a Data Controller capacity.

Transparency: The CCES shall adopt and implement an external facing privacy policy (the "CADP Privacy and Personal Information Policy") which includes the following information in clear and simple language:

(i) The purposes of the collection of Personal Anti-Doping Information from individuals interacting with the CCES through the CADP and/or other WADA-compliant anti-doping programs;
(ii) How the information is collected;
(iii) The rights of access and rectification for such individuals;
(iv) The individuals' right to withdraw consent to the communication or use of the Personal Anti-Doping Information collected; and,
(v) When applicable, the CADP Privacy and Personal Information Policy shall also identify the Third Parties for whom Personal Information is being collected by the CCES and of the possibility that the information could be communicated outside of Canada. The CADP Privacy and Personal Information Policy shall be easily available and posted on the CCES website at all times.

Consent: Pursuant to this Privacy Policy, the CCES will only use or disclose Personal Anti-Doping Information for the anti-doping purposes for which it was collected unless the individual concerned has provided their consent or as authorized by relevant data protection laws or the World Anti-Doping Code. CCES shall obtain express consent for Processing Sensitive Personal Anti-Doping Information.

Purposes of Processing: Pursuant to this CADP Privacy Policy, the CCES will only process Personal Anti-Doping Information for anti-doping purposes to fulfill the CCES Privacy Obligations.

Sharing Personal Anti-Doping Information: The CCES Contributors will not transfer Personal Anti-Doping Information to a Sub-Processor/service provider unless the Sub-Processor/service provider's handling of the Personal Anti-Doping Information is governed by an appropriate contract as per Section 1.8 of this Privacy Policy. Any request from a regulator, government authority, law enforcement or other third party seeking to obtain Personal Anti-Doping Information held by the CCES shall be immediately transmitted to the Privacy Officer who will answer such request in compliance with Section 1.5 and 1.10 of this Privacy Policy.

Processing Personal Anti-Doping Information as Data Processor

Data Processing Agreement: The CCES will only Process Personal Anti-Doping Information entrusted by Partners (who are typically WADA International Standard for Testing and Investigations Testing Authorities) for specific projects in accordance with a written agreement which shall provide at minimum (i) an obligation for the CCES to only use the Personal Anti-Doping Information for the purposes of rendering the services to the Partner, and to not keep such information after the expiration or termination of the contract, subject to legal retention requirements; (ii) an obligation for the CCES to protect such Personal Anti-Doping Information with adequate security measures (see Section 1.9) and (iii) an obligation for CCES to notify the Partner without delay of any Security Breach.

Use of template: A template Data Processing Addendum (the "**DPA template**") shall be attached to Service Agreements with Partners. The internal CCES team responsible for the contractual arrangement with the Partner will require that this DPA template be entered into or, alternatively, that an equivalent document prepared by the Partner and acceptable to the CCES be executed by the parties.

2.10 Retention and Disposal of Personal Information

General Retention Requirements: Personal Anti-Doping Information managed by the CCES as a Data Processor shall be retained in accordance with the contract in place and instructions provided by the relevant Partner. Personal Anti-Doping Information managed by the CCES as Data Controller shall be retained in accordance with this section and Part II of the Privacy Policy.

Retention Periods CADP: The CCES retains Personal Anti-Doping Information as long as necessary for fulfillment of the WADA ISPPPI purposes for which the information was originally collected by the CCES and in compliance with ISPPPI Annex A. More specifically, subject to the sub-section titled "Suspending the Destruction or Disposal of Records", records comprising Personal Anti-Doping Information shall not be kept for longer than the applicable retention period assigned to that specific record.

- **Partners:** Partners' Personal Anti-Doping Information will usually be kept for the duration of the business relationship and for a minimum period of 3 years following the end of such relationship.
- **Security Breaches:** the details pertaining to a Security Breach (see Section 1.9 of this Privacy Policy for details) will be kept for a minimum period of 2 years following the breach.
- **Access requests:** After having processed and answered an access request as per Section 1.7, CCES will retain the following information for a minimum period of 3 years: the date and nature of the request, the manner in which the request was made, the date and nature of CCES's response and if applicable, the basis for denying the request in whole or in part. To the extent that CCES denies an access or rectification request, in whole or in part, it will retain the information concerned, subject to any longer retention period provided under this Privacy Policy, for such time as is necessary to allow the person who made the request to exhaust the resources provided by law, which in most cases is 30 days.

Destruction: Under the CADP, when the CCES is no longer required to retain Personal Anti-Doping Information, the CCES will securely destroy or erase the information or make the information

anonymous. The Executive Director, Corporate Services, shall make the appropriate arrangements so that records comprising Personal Anti-Doping Information that have attained the length of retention prescribed in this Privacy Policy during the prior calendar year be, as appropriate depending on the format of the records, erased in a secure manner by overwriting in collaboration with the IT department or shredded. The CCES employees shall comply with such requirements, including by using secure methods when performing authorized destruction of Personal Anti-Doping Information. (WADA ISPPPI Annex A).

Suspending the Destruction or Disposal of Records: There are some instances where records containing Personal Anti-Doping Information will be held beyond the established retention period because of a complaint against the CCES, a privacy request, an audit, active litigation, an ongoing sanction, or the possibility of litigation that either does or may involve the CCES. The CCES will immediately suspend the application of a record retention schedule to, and the destruction of, a record or class of records:

i) Upon becoming aware, by any means whatsoever, of an allegation, claim, audit, investigation, proceeding, whether threatened, commenced, or pending against the CCES, including any employee or manager at the CCES for work performed in the course of their duties, provided such claim, audit, investigation or proceeding is either filed or appears imminent,

ii) Where required by law or by order of a tribunal, and,

iii) Where it is necessary to permit the CCES to pursue available remedies or limit any damages that it may sustain. Destruction will be reinstated upon conclusion of the investigation, in accordance with the relevant statute of limitation period, which in most cases is two (2) years.

2.11 Security

The CCES Privacy Officer is accountable for compliance with the ISPPPI.

The CCES shall at all times protect Personal Anti-Doping Information by applying all necessary security safeguards, including physical, organizational, technical, environmental and other measures to prevent the loss, theft or unauthorized access, destruction, use, modification or disclosure (including disclosure made via electronic network) of the Personal Anti-Doping Information.

The CCES shall apply security measures that take into account the risks associated with the processing of Personal Anti-Doping Information and the sensitivity of the Personal Anti-Doping Information that is to be protected.

When the CCES discloses Personal Anti-Doping Information to third party agents in connection with their anti-doping activities under the CADP or the Code, the CCES shall take all reasonable steps to ensure that such third parties use the Personal Anti-Doping Information in accordance with the laws of the country in question or, if no law is in place, with the ISPPPI.

2.12 Retention

The CCES shall ensure that Personal Anti-Doping Information is only retained for as long as is necessary to fulfil its obligations under the CADP or where otherwise required by applicable law.

The CCES will respect the retention times for different types of Personal Anti-Doping Information as may be determined by WADA from time to time unless such retention times are in breach of applicable law. In the case of TUEs, certificates will be maintained for 10 years post expiration to ensure the TUE certificate is retained for any sample being stored for later re-testing.

Once Personal Anti-Doping Information no longer serves the above stated purposes, it will be deleted, destroyed or permanently anonymized.

PART III: CSSP SPECIFIC PRIVACY POLICY

3.1 Summary

The CCES is committed to ensuring that individuals feel safe when coming forward with a Report (as defined below) of maltreatment. Part of this is understanding how we will keep your sensitive information secure. This Policy is about your rights pertaining to your information.

When the CCES receives a Report of maltreatment, it collects personal information about the person making the report (if given), the person the report is about and, sometimes, about affected parties. In some instances, some or all of those individuals may be minors. Our commitments to those who we hold personal information about:

- We will keep your information safe.
- We will explain why we need the information before you give it to us.
- We will only use your personal information for the purpose you gave it to us.
- We will not sell your information.
- We will not share your personal information without your agreement, unless necessary. For example, if necessary for reasons of safety, to enforce a *Provisional Measure,* to investigate the *Prohibited Behaviour*, or to enforce a sanction, or if required by law.
- We will use your information as part of an anonymized database to track and evaluate our work and the landscape of maltreatment in sport in Canada.

Part of ensuring that your information is safe is making sure we both understand why you are providing your personal information to us, how it will be used and how we will keep it safe. This Policy provides a fulsome explanation of how the CCES collects, uses, retains, safeguards, discloses and disposes of your Personal Information in the context of the Canadian Safe Sport Program (CSSP), and it should be read and understood in the context of and alongside the CSSP itself. Defined terms in this Part should be given the same meaning as in the CSSP, unless expressly stated otherwise.

For any questions or concerns relating to your personal information, please contact the CCES Privacy Officer: privacy@cces.ca.

3.2 Scope of CSSP Application

This privacy policy applies to all Participants who are subject to the CSSP Rules and their application.

3.3 Disclaimer

The CCES educates Parties and witnesses on the confidentiality requirements of the CSSP and the Universal Code of Conduct to Prevent and Address Maltreatment in Sport (UCCMS). However, the CCES cannot be held responsible for the conduct of the Parties or witnesses involved in the CSSP process which may cause unlawful disclosure of Personal Information that forms part of the evidentiary record before CCES.

In delivering certain services virtually, the CCES 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.

3.4 Background

The UCCMS commits the Canadian sport sector to advancing a respectful sport culture that delivers quality, inclusive, accessible, welcoming and safe sport experiences. The CSSP is similarly committed to advancing this fundamental goal.

The CSSP recognizes the CCES as the body mandated to independently administer and enforce the UCCMS for Sport Organizations, by receiving and responding to Reports of Prohibited Behaviour, and by developing and carrying out education, prevention and policy activities, including sport environmental assessments.

Part III of the CCES's Privacy 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 fair information principles outlined in the Personal Information Protection and Electronic Documents Act.

The purpose of this Policy is to describe the way the CCES collects, uses, retains, safeguards, discloses and disposes of Individual's Personal Information in the context of the CCES's role as defined in the CSSP.

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

3.5 Definitions

The following definitions are specific to Part III. All capitalized terms in Part III but not otherwise defined shall have the same meaning as defined in the CSSP Rules.

Authorized Representative: any lawyer or 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 representing a party to a CSSP process.

Document Management Program: the software platform used by the CCES in the management of documents for CSSP proceedings and/or its business operations.

Report: a submitted report intake form or information expressly deemed by the CCES to constitute a report.

CSSP Case Management Program: the software platform used by the CCES in the management of Reports to share information internally and with the Contractors to receive the information.

Contractor: any person retained by the CCES to execute tasks in the conduct of its operations in exchange for monetary compensation or co-op education credits, including those individuals under employment contracts with the CCES.

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

Implied Consent: consent that can be reasonably inferred in the circumstances from an Individual's actions or inaction.

Individual: a person whose Personal Information is collected, used, disclosed or retained by the CCES including, but not limited to Party(ies).

Party(ies): A Reporting Person, a Respondent, an Interested Party, each as defined in the CSSP.

This Policy applies regardless of how Personal Information is recorded (for example, electronically, or on paper). This Policy does not cover any information about more than one individual where the identity of the individuals is not known and cannot be inferred from the information ("Aggregated Information"). The CCES retains the right to use Aggregated Information in any way that it reasonably determines is appropriate. This Policy also does not apply to information about companies or other legal entities.

3.6 Accountability

CCES is committed to protecting Personal Information. CCES requires all Contractors, employees and others who provide services in connection with the delivery of services to comply with the obligations set out in the Policy.

3.7 Identifying Purpose and Type of Information Collected

Types of Information Collected

i) The CCES collects Personal Information that is reasonably necessary for its operations and/or required by law. This includes the categories of information described below as well as any other Personal Information volunteered to the CCES.

ii) The CCES's operations requests last names, given names, and contact information (email address and/or telephone number), confirmation of identity or authority of Contractors, Parties and, if applicable, their Authorized Representatives.

iii) The CCES receives Personal Information from the Parties or their Authorized Representatives through the initial complaint/Report, investigation, evidentiary record, submissions and other steps taken and documents received in the course of the processes set out in the CSSP. This information may include, but is not limited to, health information, criminal offences, last name, given name, contact information, and information relating to Reports against individuals and related sanctions. Personal Information provided by the Parties or their Authorized Representatives, including without limitation, financial information, health information, last name, given name and contact information, information regarding Reports or other information about procedures before the CCES, may also be collected in order to determine the admissibility to certain programs offered by the CCES (e.g., mental health referrals) and in order to offer such programs to the eligible Parties.

iv) The CCES collects Personal Information from its Contractors which includes, but is not limited to, financial information, last names, given names and contact information.

v) The CSSP Case Management System may collect cookies on user accounts such as IP addresses, sections of portal visited, and information downloaded.

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

vii) In some cases, the CCES collects Personal Information from regulatory and legal authorities, other organizations with whom the CCES or Individuals have dealings, such as government agencies, credit reporting agencies, recruitment agencies, information or service providers, and from publicly available records. The CCES may also collect information from third parties or public sources in the context of an investigation or CSSP process.

3.8 Purpose

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

The CCES will inform the Individual of the purposes for collecting and using their Personal Information by referring them to this Policy at or before the time of collection.

The CCES will not sell any Personal Information obtained.

3.9 Obtaining Informed Consent

When to Seek Consent

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

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

3.10 Express and Implied Consent

An individual or their Authorized Representative's provision of Personal Information to the CCES means that they agree to the collection, use and disclosure of their Personal Information under this Policy. If they do not agree to these terms, they shall not provide any personal information to the CCES. However, while providing some Personal Information to the CCES is optional, certain services can only be provided if the Individual's Personal Information is provided and the CCES may not be able to deliver certain services if the Individual chooses not to provide the required Personal Information.

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 CCES 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 CCES shall seek Express Consent when the Personal Information is likely to be

considered sensitive.

3.11 Detailed Consent Procedures

Standardized Consent Forms: The CCES shall develop and utilize standardized consent forms for obtaining express consent. These forms will be available in both digital and paper formats and shall be signed by the Individual or their Authorized Representative.

Digital Consent Mechanisms: For digital interactions, the CCES will implement secure digital consent mechanisms, such as electronic signatures or checkboxes, to ensure that express consent is clearly documented.

Revocation of Consent: Individuals have the right to revoke their consent at any time. However, a request to revoke consent will not terminate a process already initiated under the CSSP. The CCES shall provide a clear process for revocation, including a standardized form and a dedicated contact point for submitting revocation requests.

3.12 Limiting Collection

Collection

The CCES shall only collect Personal Information by fair and lawful means reasonably necessary for the identified purposes.

3.13 Limiting Use: Use and Disclosure

General Principle

The CCES shall only use and disclose Personal Information for the identified purposes and such purposes shall be limited, as reasonably necessary, solely to fulfilling the necessary functions of the CCES, as set out in the terms of the CSSP.

3.14 Applications of the Principle

Last name and given name may be shared with other Parties involved in the same dispute or CSSP process and with their Authorized Representatives during a CSSP proceeding(s).

Personal Information described in section 3.7(iii) may, at the sole discretion of the CCES and/or by any Contractor in the course of an investigation, adjudication, appeal, mediation or other process under the CSSP, be disclosed in the investigation report and/or adjudicator's decision when reasonably necessary to provide reasoning for the decisions rendered or findings made.

Any Personal Information described in section 3.7(iii) that is disclosed in a decision issued by the CCES and that allows for the identification of an Individual against whom a violation has been asserted shall be published, retained and distributed in accordance with the CSSP Rules.

Personal Information described in section 3.7(iv) shall be used strictly for purposes of human resources management, governance and activities of the CCES respectively.

Where possible and if it can serve the same purpose, the Personal Information described in sections 3.7(v) and 3.7(vi) will be used in aggregate forms.

Access to, use and disclosure of Personal Information outside of CCES will be limited to the CCES's Contractors in accordance with the reasonable limits required to fulfill their duties and

responsibilities with the CCES.

Personal information that is subject to a request by an Individual or their Authorized Representative shall be retained for as long as is reasonably necessary to allow the Individual to exhaust any recourse that he/she may have, provided the request is made prior to its deletion.

Any Personal Information collected by the CCES shall be managed in accordance with the Safeguards and Security standards stated in Section 3.17.

3.15 Retention

Personal Information shall be retained for a minimum period of two (2) years and shall be retained only as long as reasonably necessary and still relevant for the purposes for which it was collected.

3.16 Accuracy of Information

The CCES will take reasonable steps to ensure that Personal Information is accurate, complete, and as up to date as is necessary for the identified purpose for which it was collected.

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

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

3.17 Safeguards and Security

General Provisions

The CCES has implemented safeguards to protect against loss, theft, unauthorized access, disclosure, copying, use or modification of Personal Information. The CCES commits to maintain those measures or equivalent ones as they may be modified from time to time.

The security methods employed by the CCES are described in the CCES IT Security Policy.

Specific Areas of Safeguarding

Access to Personal Information stored on the CCES's CSSP Case Management System and Document Management System is restricted to each employee's or Contractor's responsibilities and needs.

The CCES's CSSP Case Management System and Document Management System deploy the data protection measures outlined in the CCES IT Security Policy in Part IV.

Any necessary transfer of Personal Information held by the CCES shall be transferred through the CSSP Case Management System and Document Management System Transmission of Personal Information via email will be avoided, where possible. All transmissions of Personal Information will be in non-downloadable, non-printable formats. Documents sent via email shall be password protected. A password will not be sent within the same email as the password-protected document.

Privacy Education, Training and Agreements

All employees and Contractors are made aware of the importance of maintaining the security and confidentiality of Personal Information by the CCES.

All employees and Contractors shall execute an agreement which binds them to this Policy and the relevant provisions of the policy under which the Reports(s) they are addressing are administered.

Parties and their Authorized Representatives are bound by the relevant provisions of the CSSP and the UCCMS 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.

All employees and Contractors of the CCES shall undergo mandatory security training upon onboarding and at least annually thereafter. This training will cover the latest security threats, best practices for data protection, and the CCES's specific security policies and procedures.

The CCES will maintain records of all security training sessions, including attendance and training materials. These records will be reviewed periodically to ensure compliance and effectiveness.

3.18 Destruction, Deletion or De-Identification

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.

3.19 Openness

Amendments

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

Discrepancies

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

3.20 Individual Access and Correction

Access and Corrections to Information

Subject to section 3.18 above:

- It is the right of any Individual to access his or her Personal Information upon written request to the Privacy Officer;
- The CCES shall also provide, upon written request, basic information regarding the use of the Individual's Personal Information, including disclosure to third parties, subject to the terms of the CSSP Rules;
- The Individual is entitled to request the correction of any demonstrable errors with respect to their Personal Information, in writing; and

- Where necessary for the conduct of its operations or the maintenance of services and benefits to the Individual, the CCES shall transmit the corrected Personal Information to Contractors and third parties with authorized access.

Identification

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.

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

Time to Respond to Request

The CCES shall respond no later than 30 days from the date of receipt of a written request by an eligible individual or their Authorized Representative.

Under reasonable circumstances including, but not limited to, requests of voluminous information, impracticable requests, or requests requiring a conversion of information, the CCES 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.

Cost

The CCES may require the Individual requesting a response to pay a cost for the response. The individual will be advised of the approximate cost and shall make payment before the requested information will be provided.

Refusing a Request

The CCES may refuse a correction request, with brief reasons, under certain limited instances including, but not limited to, where the Individual fails to provide sufficient proof that such information is incorrect, or where disclosure would be contrary to the terms or purposes of the CSSP. When it is impossible to amend a document, the correction shall be made by a note to file.

Despite a general right to access Personal Information upon request, the CCES may refuse an access request with reasons provided. That decision is for CCES to make in its absolute discretion, is final and binding, and is not subject to review or appeal.

The CCES may deny an access request in certain 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 Report;
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.

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

The CCES will be deemed to have refused an access request if it does not respond within the 30-day time limit.

Appendix A to Part III: CSSP Privacy Policy

The CCES collects Personal Information in respect of Individuals for the purposes set out in the CSSP, CSSP Rules as well as the following purposes:

From and about all Individuals:

- to assist the Individuals with administrative or technical support in the use of the CCES's Document Management System and CSSP Case Management System and services;
- to collect the Individuals' opinions and comments in regard to the CCES's operations;
- such other collections and uses of Personal Information from such persons and for such purposes for which the CCES may obtain consent from time to time; and
- as otherwise required or permitted by law.

From Individuals other than Contractors:

- to respond to the Individuals' Reports or inquiries;
- to receive, process, administer, investigate, mediate and adjudicate Reports and enforce decisions made under the CSSP. This may include publishing Personal Information on the public registry;
- 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 CSSP Case Management System and Document Management System and detect possible fraudulent attempted use; and
- for the purposes of statistical reporting.

From Contractors:

- to organize events involving their participation;
- for the purpose of recruitment for positions at the CCES;
- for the purpose of the administration of the CCES's policies and procedures regarding the training, retention and evaluation of Contractors;
- for the purposes of coaching, mentoring and professional development;
- for the purposes of managing productivity, including making accommodations and allowances;
- to refund admissible expenses incurred by Contractors in the form of invoices, receipts and travel information;
- from Third Party providers of benefits, pension arrangements and insurance and other related Contractor services, for the purpose of providing compensation and such services and fulfilling taxation requirements in respect of same; and
- 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.

PART IV: OTHER CCES POLICIES

IT Security Policy

4.1 IT Security Policy - Introduction

This Information Technology Security Policy (ISP) applies to all CCES employees, permanent and temporary, including contract employees (collectively, the "employees").

4.2 Policy Compliance

Employees shall be responsible for policy compliance as set out in section 4.3 below, however, the CCES shall ensure that all employees are aware of, review and understand both the contents and purpose of this Policy.

Breach of this Policy may lead to disciplinary action, up to and including termination.

4.3 Responsibilities

The Executive Director, Corporate Services, or their delegate, is accountable for the oversight of the CCES's compliance with this Policy, for ensuring that the CCES information technology (IT) commitments in the CCES Processor Data Processing Addendums are in place and that appropriate training is provided to employees.

Employees are responsible for:

- Keeping up to date on security responsibilities and attending the appropriate training regarding the use of IT systems.
- Following procedures that minimize the CCES's exposure to fraud, theft or disruption of its IT systems such as segregation of duties where appropriate (for instance in the anti-doping and finance departments).
- Ensuring that no breaches of information security result from their actions.
- Reporting any breach, or suspected breach of security without delay, to the Privacy Officer.
- Ensuring information they have access to remains secure.
- Cooperating with any investigation.

4.4 Keeping Information Secure

Data Breaches and Information Security Incidents

The CCES shall handle data breaches and security incidents in compliance with the Privacy Policy and applicable legislation.

Access control

Employees' access to IT systems is granted based on their role in the organization on a least privilege or "need-to-know" basis. By default, access privileges are limited to the lowest level of

access required to carry out an employee's role and duties. Employees may only access systems for which they are authorized. Multi-factor authentication is in place wherever possible.

The CCES has procedures to control access to its systems. Access privileges are modified in accordance with changes in employees' functions and revoked remotely when employees leave the CCES. Managers shall immediately advise the IT Team and the Privacy Officer of any request for changes requiring such modification/removal.

All personal identification devices, access cards, keys, passes, manuals and documents will be returned by the employee when the employees leaves the CCES.

System administrators (internal and external system administrators including bank account access and approvals) shall delete or disable all identification codes and passwords relating to employees when they leave the CCES.

Managers shall ensure that employees leaving the CCES's employment do not inappropriately copy, wipe or delete information from hard disks, or servers. Terminated employees will have their access rights removed immediately to avoid damage to CCES equipment and unauthorized access to CCES information, or disclosure or loss of CCES information.

All visitors shall be appropriately guided while at the CCES. If temporary passwords need to be issued to allow access to confidential systems, these shall be disabled when the visitor has left. Visitors shall not be afforded an opportunity to casually view computer screens or printed documents produced by any information system without authorization. CCES guest Wi-Fi will only be provided without access to the CCES shared drives.

Physical security to the CCES office area shall be provided through an access control system.

Security of Equipment

Laptops and mobile devices shall be deployed only with appropriate access protection, for example passwords and encryption. Devices shall not be left unattended in public places including in plain sight in vehicles.

Employees working from home or working remotely shall ensure appropriate security is in place at their location to protect the CCES equipment or information (e.g., locking doors, keeping equipment and information out of sight and unavailable to other users in the location).

CCES-issued equipment shall not be used by non-CCES employees.

Laptops and mobile devices shall be properly disposed of to ensure that any confidential information is irremediably and securely destroyed.

CCES employees and contractors are required to use the CCES VPN at all times. They shall avoid using public Wi-Fi networks, and minimize the use of personal hotspots, so as to prevent unauthorized access to their devices.

Security and Storage of Information

All information, whether electronic or manual, shall be stored in a secure manner appropriate to its sensitivity. Each team shall determine the sensitivity of the information held and the relevant storage appropriate to that information.

Clear Desk Policy

Employees shall clear private and confidential working documents, open files, and other paperwork from their desks, working surfaces and shelves at the end of each working day and place them securely into desk drawers and cupboards as appropriate.

Posting or Emailing Information

The most secure method of transmission will always be considered and utilized absent exigent circumstances, especially for sensitive and confidential information, such as personal information. In any physical or electronic transmission, the least amount of information necessary shall be placed in transit. The following procedures shall be adopted as appropriate, depending on the sensitivity of the information and may be adjusted in the event of exigent circumstances.

Sending information by email:

- Carefully check the recipient's email address before pressing send – this is particularly important where the 'to' field autocompletes.
- If confidential, personal or sensitive information is regularly sent via email, consider disabling the auto-complete function and regularly empty the auto-complete list. Both of these options can be found in Outlook under 'file,' 'options,' and 'mail.'
- Be careful when replying 'to all' – make sure you know who all recipients are and that they all need to receive the information you are sending.
- Where appropriate, use password protection, encryption technologies and secured channels when transferring sensitive information to outside parties (e.g., using Sharefile).
- Double check that any private or confidential information is removed that should be removed.

Sending information by post:

- Check that the address is correct.
- Ensure only the relevant information is in the envelope for the attention of the addressee and that someone else's letter has not been included in error.
- Label outside of the envelope "Confidential."
- If the information is particularly sensitive or confidential, consider using more secure method of delivery with reception (e.g., registered mail or courier).

Printing, Photocopying and Scanning:

- Employees shall remove all documents containing confidential information from printers, photocopiers and scanners. Employees will not leave the printer, photocopier or scanner unattended when printing, photocopying or scanning confidential information.
- When scanning, employees shall cut and paste the scan from the scan drive into the appropriate shared drive location as soon as possible. Employees shall re-check whether it is the correct scanned file prior to sending it to any external source.

Retention and Disposal of Information

The CCES disposes of information in accordance with this Privacy Policy.

Paper files containing confidential information will be shredded. Electronic information will be permanently destroyed, meaning deleted in a manner which prevents any form of non-forensic recovery.

4.5 Information and Communications Technology Security

Cloud Storage Solutions

Employees shall not use personal cloud storage solutions (OneDrive, Dropbox, iCloud, etc.) to store CCES information.

Systems Development

All system developments shall consider security issues. Where appropriate, employees shall seek guidance from the Senior Manager, Technology.

Third-party security assessments may be carried out prior to the purchase of any new system which will be used for storing and accessing confidential information.

Network Security

The CCES implements controls to prevent, detect and respond to unauthorized activity on its network, including viruses and malware, by using up-to-date technologies such as firewall, intrusion prevention and detection, web content filtering, email content filtering, and anti-malware.

The CCES may engage a third-party specialist to review network security.

Employees who believe they may have received a virus or malicious email shall report it to the IT Team.

Access Control to Secure Areas - Secure areas include:

- Server room: All corporate servers and network equipment are in a secure server room with restricted access
- Iron Mountain records
- Permanently locked file cabinets (HR files, File cabinet 4)

Security of Third-Party Access

Third parties shall only be given access to CCES networks if they are granted formal authorization by the Senior Manager, Technology, and after having signed a security and confidentiality agreement.

All third parties processing personal information on CCES's behalf (including via a hosted IT system) are required to sign a confidentiality agreement which will include data processing specifications prior to accessing the information.

The CCES has in place and shall maintain adequate policies and procedures to ensure the protection of all information being sent to external systems as well as security controls to govern the activities of such third parties.

All third parties are held to the same level of confidentiality as CCES employees.

Data Backup

The CCES has backup processes in place to ensure appropriate archiving and contingency recovery of CCES data. CCES data is held on a network directory to ensure routine backup processes capture the data.

Backups are stored on-site and at an undisclosed off-site location and are protected in accordance with the same security levels as live data. Procedures are in place to recover backups as necessary and to allow the CCES to continue its operations in the event of an emergency.

If live data is corrupted, any relevant software, hardware and communications facilities will be checked before using the backup data to ensure that backup data is not also corrupted or compromised.

Software

Employees shall only install software approved by the IT Team on CCES equipment. This is protected by restricting local administrator access.

Where the CCES recognizes the need for specific specialized hardware or software, such products shall be purchased, installed and tracked by the IT Team.

Software packages shall comply with and not compromise CCES security standards.

Use of Removable Media (for example, USB Sticks)

CCES employees shall only use authorized removable media devices. The use of removable media devices will only be approved if a valid business case for its use is developed, presented and approved by the IT Team.

Timeout Procedures

Inactive computers are set to time out after a pre-set period of inactivity. The time-out facility shall clear the screen. In high-risk areas the time-out facility shall also close both application and network sessions. A high-risk area might be a public or external area outside the control of CCES security management. The time-out delay shall reflect the security risks of the area.

Users shall always 'lock' their computers if leaving them unattended for any length of time. For high-risk applications, connection time restriction shall be considered. Limiting the period during which the computer has access to IT services reduces the window of opportunity for unauthorized access.

System Documentation

All systems shall be adequately documented and updated by the System.

The requirements in the CCES Processor DPAs will be maintained by the Senior Manager, Technology.

Version Control

Version number	Date	Approved by
1	January 1, 2025	Jeremy Luke

CONFIDENTIALITY POLICY

4.6 Confidentiality Policy - Background

The Canadian Centre for Ethics in Sport (the "**CCES**") is committed to ensuring that individuals feel safe when coming forward with a Report of maltreatment while also understanding the confidentiality obligations of all involved in the Canadian Safe Sport Program (the "**CSSP**").

The CSSP is a confidential process involving some or all of the following individuals: the Reporter, the Interested Party, the Respondent and the witnesses. Reports to the CCES are treated as confidential but there are limits to the confidentiality as described in the CSSP and UCCMS. This Confidentiality Policy (the "**Policy**") supplements the CSSP and the UCCMS. It is meant to be read together with and not supersede either document. In the event of any conflict, the CSSP governs.

4.7 Application

This Policy applies to all individuals and organizations involved in a CSSP process. This includes without limitation the Reporter, the Respondent, the Interested Party(ies), the witness(es), the Sport Organization, the independent investigator, and the contractors and employees of CCES participating in the administration of the Report.

Reporting Persons and/or Impacted Persons, Respondents, witnesses and/or other person(s) involved in a CSSP process must keep confidential all information received from another party, Sport Organization or witness, except as required by the CCES, under this CSSP, or by law. The purpose of this confidentiality provision is to maintain the integrity of all CSSP resolution or investigation processes in response to the Report.

The confidentiality obligations set out in this Policy and the CSSP exist for the duration of a CSSP investigation and resolution process. However, once the process has concluded, there is nothing that prevents a Reporter, Interested Party, Respondent or witness from speaking about their own lived experiences, including discussing the Reported incident, their experiences participating in the CSSP process, or the outcome. For greater clarity, nothing in this Rule protects any person who shares information from the operation of defamation or other applicable laws.

Note: Information that is on the *Public Registry* is public and not confidential.

4.8 Definitions

All capitalized terms in the Policy have the same meaning as defined in the CSSP Rules. To ensure that any changes made to the CSSP Rules are duplicated in this Policy, the definitions will not be reproduced here. However, those definitions are outlined in the CSSP Rules.

4.9 Obligations

Reports to the CCES are confidential.

The limit to this confidentiality is that the CCES will make all reasonable efforts to protect the privacy of individuals involved in the administration of the Reports, while balancing the need to gather information to assess and/or investigate a Report and to implement the CSSP in a manner that is procedurally fair.

Sharing of information by the CCES will be limited.

Only those individuals the CCES deems as required to know the information to implement the CSSP will receive the information. This can include CCES employees and contractors participating in the administration of the Report, legal counsel, the Reporter, the Interested Party, the Respondent, witnesses, and relevant Sport Organization(s).

The CCES may be required and/or may elect to share some or all of the following information in accordance with the CSSP and/or other legal obligations:

i) The name of the Reporter, Interested Party, Respondent and/or witnesses, depending on the anonymity elections and requests made balanced with procedural fairness (as described above);

ii) The allegations advanced against the Respondent;

iii) Information or documents obtained in the course of an investigation;

iv) The findings of fact made involving the Respondent;

v) The findings of violation made against the Respondent; and

vi) The sanctions imposed against the Respondent.

All individuals who receive information through the CSSP process will keep the information they received confidential.

The exception is that individuals may share information as required by the CCES, under the CSSP or by law.

None of the confidentiality provisions prevent Reporters, Respondents, Interested Parties or witnesses from confidentially speaking to health care providers, legal counsel, emotional support people or law enforcement.

The CCES may be required to share the information they receive in a Report with local law enforcement and/or child protective services if they are required to do so under legislation pertaining to a Duty to Report.

All documents which are created during the CSSP process, and their content, are confidential.

This includes but is not limited to, the Investigation Report, Letters of Concern, written submissions, documents pertaining to Remedial Resolution and decision letters issued by the CCES.

All documents created during the CSSP process will not be disclosed outside of the CSSP or Safeguarding Tribunal or Appeal Tribunal process except as required by law or as authorized by the CCES or a Tribunal of the SDRCC.

The integrity of the process can be impacted by any breach of confidentiality.

The individuals who are involved in the CSSP process, including the Reporter, Respondent, Interested Party(ies) and witnesses, shall not discuss or disclose any information with/to one another or with others (including on social media or publicly) during the process. Doing so can impact the credibility and reliability of information shared and can significantly interfere with the progress of an investigation and with the findings of the investigator.

4.10 Enforcement

Any breach of this Confidentiality Policy can give rise to an investigation under the CSSP and can result in sanctions as described in the CSSP.

The enforcement of the confidentiality obligations contained within the Policy is the responsibility of the CCES. Where an allegation is presented against an employee of the CCES, a third party will be responsible for administering the process against the CCES employee in accordance with the Policy.

4.11 Policy Awareness and Training

All individuals and organizations subject to this Policy will be provided a copy or reference to this Policy at the earliest reasonable opportunity.

All individuals and organizations involved in the CSSP process and subject to this policy will familiarize themselves with this Policy and review it regularly.

The CCES will provide regular training on its confidentiality policies to ensure all parties subject to the Policy understand their obligations and the importance of maintaining confidentiality.