

OWN THE PODIUM (“OTP”) Privacy Policy

Introduction

1. OTP is committed to protecting the privacy of personal information which the organization collects, holds and administers. Personal information is information which directly or indirectly identifies a person.
2. OTP’s Board is responsible for developing, adopting and reviewing this policy.
3. OTP’s CEO is responsible for the implementation of this policy, for monitoring changes in Privacy legislation, and for advising on the need to review or revise this policy as and when the need arises.

Purpose

4. The purpose of this policy document is to provide a framework for OTP in dealing with privacy considerations.

Policy

5. OTP collects and administers a range of personal information for the purposes of delivering its mandate. The organization is committed to protecting the privacy of personal information it collects, holds, and administers.
6. OTP recognizes the essential right of individuals to have their information administered in ways which they would reasonably expect – protected on one hand and made accessible to them on the other. These privacy values are reflected in and supported by our core values and philosophies and also reflected in this *Privacy Policy*, which is aligned with the *Personal Information Protection and Electronic Documents Act (PIPEDA)*. This policy will be adjusted in accordance with provincial/territorial legislation.
7. OTP has adopted the following principles as minimum standards in relation to handling the collection, use, disclosure and safeguarding of personal information. These principles will serve to shape stakeholder expectations around how OTP handles private information.
8. OTP will:
 - Collect only information which it requires for its primary function;
 - Ensure that stakeholders are informed as to why OTP collects the information and how the information gathered is administered;
 - Use and disclose personal information only for OTP’s primary functions or a directly related purpose, or for another purpose with the person’s consent;
 - Store personal information securely, protecting it from unauthorized access; and
 - Provide stakeholders with access to their own information, and the right to seek its correction.
9. With respect to staff, OTP will keep employee’s personal information confidential. Personal information includes any factual or subjective information, recorded or not, about an identifiable individual. The type of information collected by OTP that fits this definition includes:

- Name, home address, home phone number (including personal cell phone number), date of birth, dependent's age and name, ID numbers (SIN and Driver's License numbers), income, banking information, work and education history, health card number, emergency contact information, benefit pay information, performance evaluations and disciplinary notes.

Privacy Procedures:

Access to Personnel File

10. An employee's supervisor, Manager of Operations and Administration, Payroll Personnel, CEO and Vice President of Partnerships, Finance and Administration, as well as the external auditors shall have access to employee records for the purpose of carrying out their job without the consent of the employee. Personal information required by federal and provincial law, court orders or subpoena, or for legitimate business purposes, including administration of benefit plans, will be disclosed without the employee's consent, unless such consent is required by law.
11. Operations Staff keep paper files on the employee with information relevant to their specific area in locked files. There is also an electronic database which contains employee information. Access to this system is controlled by Operations and requires login and password to access.

Requesting Access to Personnel File

12. Employees may request access to review their file by making arrangements with the Vice President of Partnerships, Finance and Administration. Employees shall provide at least twenty-four hours notice (one full business day) in order to access their file. Employees may obtain a copy of any document in their file which they have signed previously and a copy of any document containing personal information that they have a right to access by law. No material contained in the employee file may be removed and viewing of the information in the file will be done under the supervision of the Vice President of Partnerships, Finance and Administration.
13. In order for OTP to ensure that the personal information maintained by Operations is accurate, complete and up-to-date, the employee must provide timely notification to Operations of any changes or corrections to their personal information.
14. The employee's file and the contents contained within are the property of OTP. An employee who leaves the organization either voluntarily or involuntarily will no longer be permitted access to their personnel file.

Third Party Release of Information

15. Human Resources and Payroll are jointly responsible for the personal information collected from all employees.
16. If an employee requires disclosure of their personal information to a third party (i.e., bank) the request must be accompanied by a completed, signed and dated Authorization to Release Information Form as provided by the requesting third party.

Internal Complaints Process

17. Employees who have concerns regarding how their personal information is stored, handled or released may contact the Vice President of Partnerships, Finance and Administration or their respective Director.
18. Any violation of this Policy that may be considered “Prohibited Behaviour” or “Maltreatment” (defined in the UCCMS and/or the Code of Conduct and Ethics) when the Respondent is an Organizational Participant who has been designated by OTP as a UCCMS Participant, will be handled pursuant to the policies and procedures of the Office of the Sport Integrity Commissioner (“OSIC”), subject to the rights of the OTP as set out in the *Code of Conduct and Ethics* and any applicable workplace policies.

Collection

19. OTP will:
 - Only collect information that is necessary for the performance and primary function of OTP.
 - Notify stakeholders about why OTP collects the information and how it is administered.
 - Notify stakeholders that this information is accessible to them.
 - Collect personal information from the person themselves wherever possible.
 - If collecting personal information from a third party, be able to advise the person whom the information concerns, from whom their personal information has been collected.
 - Collect Sensitive information only with the person’s consent. (Sensitive information includes health information and information about religious beliefs, race, gender and others).
 - Determine, where unsolicited information is received, whether the personal information could have been collected in the usual way, and if it could have, it will be treated normally. (If it could not have been, it must be destroyed, and the person whose personal information has been destroyed will be notified about the receipt and destruction of their personal information).

Use and Disclosure

20. OTP will:
 - Only use or disclose information for the primary purpose for which it was collected or a directly related secondary purpose.
 - For other uses, OTP will obtain consent from the affected person.
 - In relation to a secondary purpose, use or disclose the personal information only where:
 - a secondary purpose is related to the primary purpose and the individual would reasonably have expected OTP to use it for its purposes; or
 - the person has consented; or
 - certain other legal reasons exist, or disclosure is required to prevent serious and imminent threat to life, health or safety.
 - Provide all individuals access to personal information except where it is a threat to life or health or it is authorized by law to refuse and, if a person is able to establish that the personal information is not accurate, then OTP must take steps to correct it. OTP may allow a person to attach a statement to their information if OTP disagrees it is inaccurate.
 - Where for a legal or other reason OTP is not required to provide a person with access to the information, consider whether a mutually agreed intermediary would allow sufficient access to meet the needs of both parties.
 - Make no charge for making a request for personal information, correcting the information or associating a statement regarding accuracy with the personal information.

Storage

21. OTP will:

- Implement and maintain steps to ensure that personal information is protected from misuse and loss, unauthorized access, interference, unauthorized modification or disclosure.
- Before OTP discloses any personal information to an external recipient including a provider of IT services such as servers or cloud services, establish that they are privacy compliant. OTP will have systems which provide sufficient security.
- Ensure that OTP's data is up to date, accurate and complete.

Destruction and de-identification

22. OTP will:

- Destroy personal information once it is not required to be kept for the purpose for which it was collected, including from decommissioned laptops and mobile phones.
- Change information to a pseudonym or treat it anonymously if required by the person whose information OTP holds and will not use any government related identifiers unless they are reasonably necessary for OTP functions.

Data Quality

23. OTP will:

- Take reasonable steps to ensure the information OTP collects is accurate, complete, up to date, and relevant to the functions OTP performs.

Openness

24. OTP will:

- Ensure stakeholders are aware of OTP's *Privacy Policy* and its purposes.
- Make this information freely available in relevant publications and on the organization's website.

Access and Correction

25. OTP will:

- Ensure individuals have a right to seek access to information held about them and to correct it if it is inaccurate, incomplete, misleading or not up to date.

Anonymity

26. OTP will:

- Allow people from whom the personal information is being collected to not identify themselves or use a pseudonym unless it is impracticable to deal with them on this basis.

Making information available to other organizations

27. OTP can:

- Release information to third parties where it is requested by the person concerned.

Last Updated : January 13, 2023