Title	Effective Date	Page
Confidentiality and Privacy	**February 11, 2017**	**1 of 8**
Policy Number	**Updates and Replaces**	
GP 6	**March 19, 2011**	
	Next Review Date	
	February 2020	

POLICY STATEMENT

The purpose of this policy is to govern the collection, use and disclosure of personal information in the course of business in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of the Association to collect, use or disclose personal information.

1. The Association will take all reasonable steps to maintain the confidentiality of all confidential Association and personal information.

2. The Association will respect and protect the privacy of personal information by complying with the 10 privacy principles required by the Personal Information Protection and Electronic Documents Act (PIPEDA), as follows (refer to Attachment A):
    a. Accountability.
    b. Identifying purpose.
    c. Consent.
    d. Limiting collection.
    e. Limiting use, disclosure and retention.
    f. Accuracy.
    g. Safeguards.
    h. Openness.
    i. Individual access.
    j. Challenging compliance.

3. The Association will maintain a privacy policy for distribution to members, clients and other interested parties, and will post this policy on its website. The policy will include references to:
    a. Restrictions placed on that disclosure.
    b. Time limits for holding personal information collected and the commitment to destroying unneeded information.
    c. The process by which individuals may access their personal information.
4. The Association's current policy is under Attachment B

Title	Effective Date	Page
Confidentiality and Privacy	**February 11, 2017**	**2 of 8**
Policy Number	**Updates and Replaces**	
GP 6	**March 19, 2011**	
	Next Review Date	
	February 2020	

5. The Association will maintain high standards of physical and electronic security wherever personal information is being handled.

6. The Association's Privacy Officer can be reached at:

   Privacy Officer
   Ontario Tennis Association
   1 Shoreham Drive, Suite 200
   Toronto, ON M3N 3A7
   416 514-1100
   privacy@tennisontario.com

   All requests for access to personal information and all contact with the Privacy Commissioner of Canada will go through the Privacy Officer.

7. Employees have a right to understand, access and correct their personal information. Employee personal information collected, used or disclosed will be subject to the same care and conditions as outlined for other personal information.

PURPOSE

1. This Statement of Policy and Procedure outlines the Association's compliance with privacy legislation, principles and practice.

SCOPE

1. This policy applies to all Association employees, Directors and volunteers.
2. Compliance with the principles outlined in this policy shall be treated as essential for contract compliance with suppliers, consultants and other contracted organizations.

Title	Effective Date	Page
Confidentiality and Privacy	**February 11, 2017**	**3 of 8**
Policy Number	**Updates and Replaces**	
GP 6	**March 19, 2011**	
	Next Review Date	
	February 2020	

RESPONSIBILITY

1. It is the responsibility of every employee to ensure that privacy of personal information is protected and respected.
2. It is the responsibility of the Privacy Officer to:
    a. Develop and maintain both internal and external privacy policies.
    b. Ensure that systems and processes are in place to support the policies.
    c. Act as an expert resource on privacy within the Association.
    d. Act as a point of contact on privacy issues.

DEFINITIONS

1. "**PIPEDA**" is the Personal Information Protection and Electronics Document Act, the Canadian law governing the commercial collection, use and disclosure of personal information.
2. "**Personal information**" refers to all information related to a unique individual including name and contact information, identification numbers or codes, and sensitive personal information.
3. "**Cookies**" refers to log files planted in an individual's computer hard drive to record and save personal information about the individual's location and preferences for future use.
4. "**Privacy Commissioner of Canada**" refers to the individual who has been identified by the federal government to inform and enforce PIPEDA.
5. "**The Association**" refers to The Ontario Tennis Association (OTA), its employees, Directors and volunteers.

REFERENCE POLICIES

HR14 – Privacy Officer Roles and Responsibilities

Title	Effective Date	Page
Confidentiality and Privacy	**February 11, 2017**	**4 of 8**
Policy Number	**Updates and Replaces**	
GP 6	**March 19, 2011**	
	Next Review Date	
	February 2020	

PROCEDURE DEVELOPMENT

1. The Association will protect and respect confidential and personal information by:
    a. Taking all reasonable steps to secure and protect the information, as follows:
        i. Electronic records of personal information will be subject to limited access by authorized personnel in the performance of their duties.
        ii. Printed records of personal information, when they are not under the control of authorized personnel, will be kept in a secure location.
    b. Disclosing to individuals that personal information is being collected and directing them to the Privacy policy.
    c. Destroying the information when it is no longer required. Personal information will be destroyed two years after it is no longer required.

2. Appointment of the Privacy Officer

The Board of Directors, upon the recommendation of the President, will appoint a Privacy Officer, whose name and contact information will be publicly available as the point of contact for all inquiries or issues related to privacy of personal information.

3. Detailed Guidelines

a. Personal information may be collected without knowledge or consent only in the following circumstances:
    i. In the event of an emergency that threatens the life, health or security of an individual.
    ii. If there are reasonable grounds to believe that the information could be useful to investigate the contravention of a law.
    iii. The collection is in the interest of the individual and consent cannot be obtained in a timely way.
    iv. The collection of the information with the individual's knowledge or consent would compromise the availability or accuracy of the information and the collection is required to investigate the contravention of a law.
    v. The information is publicly available.
b. Personal information may be disclosed without knowledge or consent only in the following circumstances:

i. In the event of an emergency that threatens the life, health or security of an individual.
ii. To a lawyer representing the Association.
iii. To collect a debt owed to the Association by the individual.
iv. To a government institution that has indicated disclosure is required on a matter relating to national security or the conduct of international affairs.
v. The information is publicly available.
vi. If required by law.
vii. For other circumstances listed in subsection 7(3) of PIPEDA.

c. Requests from an individual to provide information about their personal information being collected, used or disclosed by the Association will be answered within 30 days. No fee will be charged for this service.

d. If an individual withdraws consent for the use of personal information, the Privacy Officer will take all necessary steps to cease the Association's use of the information within 30 days.

ATTACHMENTS

Attachment A – Ten Principles for the Protection of Personal Information
Attachment B - Privacy Policy - Internet posting

Title	Effective Date	Page
Confidentiality and Privacy	**February 11, 2017**	**6 of 8**
Policy Number	**Updates and Replaces**	
GP 6	**March 19, 2011**	
	Next Review Date	
	February 2020	

Attachment A –
Ten Principles for the Protection of Personal Information

These 10 principles are summarized from a Model Code for the Protection of Personal Information in the National Standard of Canada, based on Schedule I of the PIPEDA legislation. More explicit information can be obtained by referring directly to the Schedule.

Principle 1 – Accountability
An organization is responsible for personal information under its control and shall designate an individual accountable for the organization's compliance, whose identity should be made known upon request. The individual bears accountability for compliance regardless of who may perform related day-to-day processes. The organization is responsible for information transferred to a third party for processing and should take steps to provide a comparable level of protection of the information from that third party.

Principle 2 – Identifying Purposes
The purposes for which an organization is collecting personal information should be documented at or before the time of collection. These purposes should be specified to the individual at or before the time of collection, either verbally or in writing. Care should be taken not to collect information that isn't strictly needed. Should a new purpose arise after this, the consent of the individual is again required before it can be used, unless the use is required by law.

Principle 3 – Consent
The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where that is inappropriate. In certain circumstances, such as when medical, legal or security reasons make it impossible, personal information can be collected, used or disclosed without the knowledge or consent of the individual. An organization should not, as a condition of sale of a product or service, require consent for other uses of the information beyond that required to provide the product or service. In obtaining consent, the reasonable expectations of the individual are also relevant, as for example, an individual should reasonably expect a magazine to contact them for subscription renewals. Consent should not be obtained through any form of deception. An individual may withdraw

their consent at any time subject to legal or contractual restrictions and reasonable notice.

Principle 4 – Limiting Collection
The collection of personal information should be limited to that which is necessary for the purposes identified by the organization. Information should not be collected indiscriminately. Information should not be collected illegally.

Principle 5 – Limiting Use, Disclosure and Retention
Personal information should not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information should be retained only as long as necessary for the fulfilment of those purposes. Organizations should develop documented guidelines for the retention periods for personal information. After the retention period is up, personal information no longer required should be destroyed, erased or made anonymous.

Principle 6 – Accuracy
Personal information should be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used. Unless it is required for the original purpose, an organization should not routinely update personal information.

Principle 7 – Safeguards
Personal information should be protected by security safeguards appropriate to the sensitivity of the information. Safeguards against loss, theft, and unauthorized access, copying, use or modification should all be addressed, including physical measures (eg locks, restricted access areas), organizational measures (e.g., security clearances, authorization processes) and technological measures (e.g., passwords, encryption). The nature of the safeguards should vary with the level of sensitivity of the information. Employees should be made aware of the importance of maintaining confidentiality of personal information. Care should be used in the disposal or destruction of personal information.

Principle 8 – Openness
An organization should provide to individuals its policies and practices relating to the personal information. This includes the name or title and address of the organization's Privacy Officer, how to gain access to personal information held by the organization, a description of the type of information held and details of what information is made available to related organizations

and why.

Principle 9 – Individual Access
Upon request, an individual should be informed of the existence, use and disclosure of his or her personal information and be given access to it, within a reasonable time frame and at limited or no cost to the individual. An individual should be able to challenge the accuracy and completeness of the information and have it amended. Under certain limited circumstances (cost, references to others' personal information, legal, security, competitive proprietary, subject to litigation or client privilege) an organization may not be able to provide the information, but these situations should be limited and specific. An organization holding sensitive medical information may choose to make it available through a medical practitioner. It is fair for an organization to require specific personal information to validate a person's identity before disclosing. Organizations should be able to provide a list of other organizations to which they have disclosed personal information.

Principle 10 – Challenging Compliance
An individual should be able to address a challenge concerning compliance with the above principles to the Privacy Officer of the organization. Principles and procedures related to this principle should be in place. Complaints should be documented, investigated and responded to within a reasonable period.

APPROVALS

President		Date:
on behalf of the Board of Directors		Date: