

## Alberta Orienteering Association Privacy Policy and Anti-Spam Legislation Policy

Approved: on April 6, 2020

Updated and approved on: February 12, 2026

### AOA Privacy Policy

The Alberta Orienteering Association (AOA), as a non-profit organization registered under the *Societies Act*, and is regulated by the [Personal Information Protection Act](#) (PIPA) of Alberta.

The AOA follows the principles in Alberta's Personal Information Protection Act (PIPA) for all personal information it collects, uses, or discloses in connection with its membership, programs, events or activities.

#### What We Collect

Only necessary information:

- Members or participants: name, email, address, gender, age/DOB.
- Additional information may be collected for events and programs: vehicle licence plate number, cell phone number, or medical information (optionally provided for safety).
- Volunteers, board members, coaches, or staff: background check data (with explicit consent).

#### Purposes and Consent

We collect for:

- Membership and event registration and management.
- Program and event communication and volunteer coordination. This can include communications or newsletters tailored for participants regarding membership, programs, or events.
- Safety and emergency contact. This is ONLY used for safety management e.g. in the case of a missing or injured participant.
- Results display, name and age group may be posted publicly unless you contact AOA to opt out.
- Reporting to Orienteering Canada and the Government of Alberta for membership demographic reporting, which is primarily managed through statistical data.

#### Disclosure and Use

**By providing information, anyone who signs up for membership, events, programs, or volunteering consents to the above uses.**

### Information stays within AOA except:

- For reasonable purposes under PIPA (e.g., due to legal requirements, emergencies, or business transactions where appropriate). This information is NEVER sold.
- With Orienteering Canada, the Government of Alberta, and insurers for reporting
- For posting results: names and age group may be posted publicly unless you contact AOA to opt out.

### Access and Correction

Individuals may request access to their personal information held by the AOA and request corrections to inaccurate information. The AOA will respond within 45 days, subject to any applicable exceptions in PIPA.

**Privacy Officer Contact Information: AOA Executive Director [info@orienteeringalberta.ca](mailto:info@orienteeringalberta.ca)**

### Retention

The AOA keeps data only as needed for functional purposes or legal requirements and securely disposes of all personal information once it is no longer required. All personal information is securely stored by our secure registration systems or forms managed by the Executive Director.

## AOA Anti-Spam Legislation (CASL) Policy

Canada's Anti-Spam legislation came into effect July 1, 2014, and applies to non-profits such as the AOA and its clubs. These laws apply to commercial conduct. [Canada's anti-spam legislation](#) (CASL) protects consumers and businesses from the misuse of digital technology, including spam and other electronic messages.

**The AOA will only contact people with commercial electronic messages regarding AOA, its affiliated clubs, and orienteering-related activities (e.g., event or service promotion) if consent (implied or expressed) has been received.**

1. Consent: The AOA will have expressed or implied consent from all its contacts to receive a commercial electronic message from AOA. *Implied consent* is valid within two years of membership purchase or within 6 months of an inquiry.
2. Identification: The AOA will clearly identify itself as the organization sending the commercial electronic message in the message.
3. Unsubscribe: The AOA will include an unsubscribe mechanism on every commercial electronic message sent.

For more information about complying with this legislation, go to [www.crtc.gc.ca/antispam](http://www.crtc.gc.ca/antispam)

## Risk management processes

### **Security Risk Mitigation**

Staff, board members, and volunteers who obtain access to personal information receive periodic training on privacy and security, and they must sign the MoU ( appendix A) before accessing personal information. See the security practices included in the MoU below.

## Memorandum of Understanding for the AOA Privacy Policy

### Between

The Alberta Orienteering Association (AOA),

### and

\_\_\_\_\_ (name)

\_\_\_\_\_ (title e.g. director, volunteer coordinator, program staff etc.)  
collectively known as “the parties”

The objective of this memorandum of understanding is to clarify the roles and responsibilities of the parties in protecting personal information collected for the purpose of carrying out AOA business.

The AOA is subject to the *Personal Information Protection Act (PIPA)* and *Canada’s Anti-Spam legislation (CASL)* which sets out principles of fair information practices that in turn form ground rules for the collection, use and disclosure of personal information.

### Understanding of roles and expectations:

**The AOA ensures** that best practices regarding personal information, collection and protection are followed as stated in the Privacy Policy and CASL Policy.

- The AOA will ensure that access to personal information is limited to only those who need it.
- The AOA will ensure that everyone who has access to personal information is aware of the privacy policy and **security practices** listed below.

**Staff, volunteers, and directors ensure that they are aware** of the AOA Privacy Policy and CASL Policy and are required to **follow the AOA Security Practices** listed below.



## Protecting Personal Information for Non-Profit Organizations AOA Security Practices

**We only collect personal data that is necessary!**

- IF we keep records in paper files**
    - Locked file cabinets and desk drawers protect information in paper files.
    - Keys are only provided to staff who need access to the files to perform their work.
    - Paper files are cross-cut shredded (or otherwise destroyed) before being disposed of.
  - If we keep records in electronic form**
    - Computers are password-protected.
    - Staff must log in to access personal information.
    - Personal information is accessible only to those who need it and are allowed.
    - Computers are physically secured, e.g., doors are locked when left alone.
    - Firewalls and anti-virus software are kept up-to-date to protect against invasive malware.
    - Only secured networks are used, which have adequate encryption according to current encryption standards. This will protect personal information, along with any other confidential information of this organization. We do not use public networks when working with personal data.
    - Two-step verification (2SV) is required beyond just a password for cloud-based services (e.g. google drive, one-drive etc.)
  - We don't send or receive personal information by email**
    - We don't share email addresses unless consent is given by the person.
    - We only use secure email accounts that can be accessed by the user who owns it (no shared email accounts).
    - Any email that contains personal information data should be deleted as soon as possible when the information is no longer needed.
    - We will only contact people with **commercial electronic messages** regarding the AOA, its clubs and orienteering-related activities if consent (implied or expressed) has been received, the sender is identified, and has an "unsubscribe" mechanism.
- 
- Personal information stored on portable media devices (e.g. laptops or flash drives)**
    - Personal information is stored on portable devices, external drives, flash drives, only when necessary and only as much as is necessary for the task.

- Portable media devices must be password-protected.
  - Our volunteers and employees sometimes take files containing personal information home to work on**
    - Our policy is to only “take-home” records if necessary and with approval.
    - Staff must make sure the records are kept separate and are not accessible to other household members.
    - Staff must return or destroy the data after use at home (shredder for paper records or permanently delete files).
  - Our staff members are aware of their obligation to protect privacy**
    - Board members, employees, and volunteers who have access to personal information receive information about their obligation to protect personal data.
  - If we accept credit or debit cards for payment**
    - Point of sale is done by a secure third-party provider, and we do not have access to credit card information.
  - We post membership, team lists, team schedules, etc., on our website**
    - Consent is obtained to post names, photographs, and other personal information on our website.
  - We do not give out any information to third parties.** The only exception is to provide necessary information to government agencies and Orienteering Canada for the provision of member or participant services, for safety purposes, or to meet federal, provincial, or funding agency reporting requirements.
  - We securely dispose of all personal information once it is no longer required:** shredder for paper records or permanent deletion of files from electronic devices and cloud storages.
    - AOA staff (Executive Director) is responsible for doing a monthly scan and deletion of non-essential personal information data.
  - AOA staff (Executive Director) is the main contact person for privacy policy related requests**
- 

Name:  
Position:  
E-mail:  
Date:

\_\_\_\_\_  
(Signature)

AOA representative:  
Position: ED  
E-mail:Info@orienteeringlberta.ca  
Date:

\_\_\_\_\_  
(Signature)

**Government of Alberta** ■  
<https://www.alberta.ca/personal-information-for-non-profits-and-other-organizations.aspx>