Privacy Policy

Role and composition of the Committee on Access to Information and Privacy

The mission of the Abenaki Council of Odanak (ACO) consists in ensuring the representation of members of the Abenaki Community of Odanak and promoting the preservation of their identity, culture and quality of life.

To do so, the Council seeks to provide quality services for youth, elders and for the entire community, according to the Band's resources.

The Council is committed to transparency and equity in its decisions, while supporting individual and collective autonomy to ensure the Band's future.

Adopted, May 15, 2023

In effect, May 15, 2023

Resolution ROB-014-23-24

1. POLICY OBJECTIVE

This policy demonstrates the Abenakis of Odanak Council's (AOC) commitment to information security and the protection of personal and confidential information.

The AOC is a public body subject to the *Privacy Act* - R.S.C. 1985, c. P-21 and the *Personal Information Protection and Electronic Documents Act* (PIPEDA), among others. In addition, this policy interfaces with the policies and procedures related to information management and the governance policies and procedures under the AOC Financial Administration Act.

The Privacy Policy sets out how the AOC protects personal and confidential information and outlines standards for collection, use, communication, conservation, right of access and rectification. It also defines the role and composition of the AOC *Committee on Access to Information and Privacy*.

2. POLICY ORIENTATIONS

2.1. Protection of personal and confidential information

The AOC is committed to protect privacy and the personal and confidential information that it collects and retains, is committed to compliance with the provisions, values and fundamental principles established by applicable legislation. The AOC ensures implementation of the measures necessary to guarantee transparency and respect for the confidentiality of the information provided when services are requested.

2.2 Information security

The AOC undertakes to implement a range of technological, organizational, human, legal and ethical measures to ensure the security of information, notably:

- Information availability, where information is accessible in a timely manner, as required by authorized individuals;
- Information integrity, where information is not destroyed or altered in any way without authorization, in accordance with the AOC retention schedule, and the medium bearing such information provides the desired stability and sustainability;
- Information confidentiality, where disclosure of information is limited only to authorized individuals;
- Identification and authentication to confirm, when required, the identity of an individual or the identification of a document or device;

- Irrevocability to ensure that an action, exchange or document is clearly and undeniably attributed to the entity that generated it;
- Compliance with legal, regulatory or business requirements to which the AOC is subject.

3. DEFINITIONS

3.1. Personal Information

Any information that involves an individual and can identify him/her, subject to any exceptions provided by applicable laws. Such information may be of a personal nature, such as the individual's address, phone number, health status, lifestyle, or financial situation.

3.2 Confidential information

Any information that involves a building or corporate body and relates to information that its author or owner deems confidential due to its financial, commercial, or strategic nature, unless applicable laws in the public sector provide, by way of exception, that such information held by the AOC is public.

3.3 Information security

Protection resulting from all security measures that are implemented to ensure the confidentiality, integrity, and availability of the information that the AOC holds based on the sensitivity and value of such information, the risks to which it is exposed, and the obligations to which it is subject.

4. CONSENT, COLLECTION AND RETENTION OF PERSONAL AND CONFIDENTIAL INFORMATION

4.1. Consent and collection method

The AOC collects information in a fully transparent manner with the free and informed consent of users and only in cases where the information collected is required to provide a desired service.

In accordance with applicable laws, when the AOC collects personal and confidential information, it clearly indicates the purposes for which the

information is being collected and requests the user's consent to use such information. The AOC must obtain consent again to use previously collected information for another purpose.

Certain AOC services or activities may concern minors. In such cases, personal information is collected with the consent of the child's parent or guardian. Information is collected primarily through forms, website, telephone conversations, opinion surveys and questionnaires.

4.2 Collected information

Depending on the service provided, the AOC may collect and retain any of the following information: full name, mailing address, e-mail address, telephone numbers, fax number, credit card number, Indian status card number, hunter's license number, student identification number, driver's license number, social insurance number, health insurance number, and date of birth.

4.3 Collection of technical information during use of the website or online services

The AOC collects technical information such as IP addresses, pages visited, requests, dates and times of connection, type of Web browser or computer system used, or the names of website domains used to link up to the caodanak.com site.

When Web users use online services or visit the caodanak.com website, the AOC or its agent may also store certain information on their computers in the form of cookies or similar files. Cookies help retain certain information on use of the website or an online service. By targeting the interests and preferences of Web users, cookies enable the AOC to improve its service delivery and the client experience. Cookies may be required to meet the technological or security requirements of Web browsing or to enable an online service to run properly.

Most Web browsers allow Web users to delete cookies from their computer's hard drive, block cookies, or receive a warning before cookies are set. Web users who refuse cookies will nevertheless have access to the site, but browsing may be affected and certain services may not be available.

4.4 Purpose of collecting information

When the AOC collects and retains personal and confidential information, its objective is to offer users secure, personalized service in accordance with applicable laws and its security rules.

The AOC uses the personal, confidential or technical information that it collects for the following purposes:

- Verify the identity of users;
- Ensure that users and the AOC are protected against fraud and false statements;
- Offer personalized service delivery;
- Determine eligibility for services offered by the AOC;
- Monitor requests for services made to the AOC and its agents;
- Provide information to members on services and programs in effect;
- Compile statistics;
- Improve available services.

5. RIGHT OF RECTIFICATION, WITHDRAWAL AND DESTRUCTION

A member of Odanak may request to have their information corrected, destroyed or no longer used for the purposes for which it was collected. To do this, they must contact the department involved.

In accordance with the *Privacy Act* - R.S.C. 1985, c. P-21 and the *Personal Information Protection and Electronic Documents Act* (PIPEDA), information is retained for the period provided for on the AOC's retention schedule and classification plan and subsequently destroyed.

In accordance with applicable laws, the AOC undertakes to comply with any request to withdraw, rectify, or destroy information, subject to legal obligations to the contrary.

6. INFORMATION SECURITY

The AOC uses information technology extensively to support its business processes in order to offer service delivery consistent with its service statement. All collected personal and confidential information is retained in a secure environment. Staff and agents are required to respect the confidentiality of information.

The AOC implements appropriate, useful and necessary security and access management measures based on the sensitivity of the information processed. Only individuals who require access to personal and confidential information to perform their duties can access this information.

The AOC integrates technological innovations to ensure the confidentiality, integrity, and availability of transactions and information in its various modes of service delivery.

7. ROLES AND RESPONSIBILITIES OF THE AOC

The AOC is responsible for personal information collected, retained, used, disclosed and destroyed in the course of carrying out its mission. The AOC will continue to develop policies and practices to ensure that member information is handled in strict compliance with the *Privacy Act*. The AOC's Executive Management is responsible for overseeing the application of these policies and practices to ensure compliance, namely by:

- Providing the same training to all AOC personnel;
- Ensuring open, complete and timely communication with employees and others about the AOC's policies, practices and expectations regarding the handling of personal information;
- Ensuring that the *Committee on Access to Information and Privacy* is operational;
- Establishing standards for classifying the sensitivity of personal information to determine the appropriate level of protection for that information;
- Working with the AOC's digital information security agent to ensure that personal information is protected from loss and from inappropriate access, use, disclosure or destruction;
    - Implementing systems that ensure that only employees whose duties require access to personal information are authorized to have access to that information;
    - including specific provisions in contracts or other arrangements with third parties that require compliance with the *Privacy Act*, this policy and internal procedures;
- Ensuring that procedures are established for members to request access to and correction of their personal information and to address complaints about the management of their personal information;
- Ensuring that procedures are established to notify members of any inappropriate collection, retention, use, disclosure or destruction of their personal information;
- Monitoring compliance with this policy and, if necessary, taking action to correct any deficiencies.

Employees — Staff members who collect personal information on behalf of the AOC shall be required to explain the purpose for which the information is collected. If they are unable to do so, they shall be required to refer the member to another employee who can explain the purpose of the collection. It is the responsibility of each AOC employee to ascertain their obligations under this Policy and the *Privacy Act*. Employees must report any violations of the Policy or the *Act* to their immediate supervisor or to the AOC Executive Management. Under no circumstances shall employees disclose information to third parties without the consent of the individual concerned.

Directors – In addition to the above responsibilities, directors shall inform their employees of the requirement to comply with the Policy and the *Act*. They shall also review or investigate any matter brought to their attention regarding the Policy or the *Act*. Where appropriate, Directors should notify, work with or refer issues to the Assistant General Manager - Human Resources Manager or the AOC's Digital Information Security Agent.

Executive management — The AOC's Executive Management shall provide advice and guidance to directors and employees with respect to the AOC's handling of personal information. It shall also serve as the first point of contact for individuals seeking information or having concerns about the AOC's handling of their personal information.

Violation of this policy, whether intentional or through negligence, may result in disciplinary action up to and including dismissal or termination of association with the AOC.

Legal sanctions may also be taken, if necessary.

8. RESPONSIBILITIES OF THE ODANAK MEMBER

8.1. Members are responsible for the information that they provide to the AOC and for maintaining the confidentiality of their identification and authentication information (user codes, access codes, passwords, access cards, etc.). The AOC may not be held liable for unauthorized use caused by members.

8.2. Members must also ensure that the system or equipment they use to transmit or receive information from the AOC is sufficiently secure, and must exercise vigilance. The AOC may not be held liable for unauthorized access to information resulting from negligence or vulnerabilities present in the equipment or systems of members.

8.3. In the event that the confidentiality of their information becomes compromised or their identities are stolen, members must notify the AOC as soon as possible by contacting the department involved.

8.4. The City does not solicit members by email or otherwise to obtain personal or confidential information about them.

9. COMMITTEE ON ACCESS TO INFORMATION AND PRIVACY

9.1. Role of the Committee

The Committee provides leadership and fosters an organizational culture that emphasizes privacy and transparency.

- Support the AOC in carrying out its responsibilities and obligations;
- Setting and approving privacy policies;
- Approve governance rules;
- Advise and suggest safeguards on all information system acquisition, development and redesign projects, including video surveillance and the introduction of new technologies;
- Plan and conduct training activities;
- Promote the policies, guidelines and decisions formulated by the Access to Information Commission (Commission d'accès à l'information);
- Evaluate the level of protection of personal information on an annual basis.

9.2. Composition

- AOC Executive management;
- AOC Assistant General Manager - Human Resources Manager;
- AOC Digital information security agent;
- If necessary, any other resource whose expertise is required (internal or external).

10. RESTRICTIONS ON ACCESS TO SERVICES

The AOC reserves the right to destroy users' accounts without notice, at its sole discretion, at any time. The AOC also reserves the right to restrict users' access in whole or in part to applications offered by the AOC. The AOC may not be held liable for such suspensions, cancelations, or restrictions.

11. INCIDENT REPORTS

The AOC undertakes to inform members of incidents that affect the protection of personal information.

12. LINKS WITH OTHER SITES

The AOC website contains hyperlinks to other sites. Information exchanged on such sites is not protected by this privacy and security policy, but is subject to the policies of the external sites.

The AOC is not responsible for the content of such sites and does not endorse them. The AOC may not be held liable for any damage of any nature whatsoever that results from the navigation or use of such sites.

13. EMPLOYEES IN CHARGE OF POLICY ENFORCEMENT

Executive Management of the AOC is responsible for ensuring compliance with the privacy and confidentiality component of the policy.

The AOC agent in charge of digital information security is responsible for ensuring compliance with the policy component regarding the security of digital information.

14. ADDITIONAL INFORMATION, COMMENTS OR COMPLAINTS

For questions, comments or complaints about this policy or its application, members may contact the appropriate sector of the AOC.

If a member is not satisfied with the response, they may contact in writing AOC Executive Management:

Abenakis of Odanak Council
104 rue Sibosis, Odanak (Québec) J0G 1H0
Email: reception@caodanak.com