Concours international d'orgue du Canada

Canadian International Organ Competition

Personal Information Handling & Management Policy

Policy Brief & Purpose

The CIOC is committed to taking steps to process personal information in a manner that respects the confidentiality and sensitivity of such information, to protect the security, integrity, and accuracy of personal information, and ensuring that information is collected for appropriate reasons and purposes. The CIOC will always ensure that information is handled in compliance with applicable legal and regulatory requirements, including the *Personal Information Protection and Electronic Documents Act (Canada)* and substantially similar provincial laws (collectively "**Canadian data protection laws**"). For the purposes of this policy, the CIOC defines two roles within the organization and its handling of personal information:

1. The **Privacy Officer** is the individual tasked with the management of all personal information collected by the organization.
2. **CIOC staff** may only use personal information in order to carry out their duties, and must take appropriate safeguards to protect this information.

Roles and Responsibilities of the Privacy Officer

- Ensuring that the CIOC complies with all applicable Canadian data protection laws.
- Implementing best practices and procedures for the handling of personal information, as outlined in the CIOC's policies and procedures relating to personal information.
- Updating and revising the CIOC's policies and procedures relating to personal information as needed.
- Controlling access to personal information by designating trusted employees to process and handle personal information, and overseeing their work to ensure it is in compliance with policies and procedures.
- Training employees who handle personal information in privacy and data security.
- Developing and implementing appropriate security measures to protect personal information from theft or exposure and to prevent data breaches.
- Developing a response plan in case of a data breach.
- Evaluating new contracts related to the processing, handling, storage, or destruction of personal information by third-party service provides to ensure that contracts for these services indicate that the third-party is committed to legal and ethical practices with respect to privacy in accordance with Canadian data protection laws.
- Developing an appropriate data retention schedule.
- Conducting privacy impact assessments in accordance with Canadian data protection laws in cases where CIOC of (i) acquires, develops or overhauls an information system or an electronic service delivery system involving the collection, use, communication, keeping or destruction of personal information; (ii) intends to implement a project which could create a meaningful potential risk to the privacy interests of individuals concerned; (iii) transfers Quebec residents' personal information outside of Quebec.

- Managing and responding to requests to access or rectify information, as well as complaints related to personal information.

Roles and Responsibilities of CIOC staff

- Reviewing and complying with all CIOC policies and procedures related to privacy and personal information.
- Respecting the confidentiality and sensitive nature of personal information.
- Using information only for needed purposes, in order to complete necessary tasks to fulfill contractual obligations, administrative tasks, etc.
- Ensuring that they have permission from the Privacy Officer before accessing any records containing personal information.
- Ensuring that personal information that the staff member is working with is up-to-date, accurate, and that it is being handled in a way that prevents inaccurate, falsified, or corrupted information from circulating.
- Prohibiting the disclosure of personal information to third parties, except as required by law.
- Seeking guidance from the Privacy Officer if the staff member is unsure of their obligations under any CIOC policy or procedure with respect to personal information and privacy.
- Promptly directing requests to access or rectify personal information, or withdraw consent, as well as complaints to the Privacy Officer.
- Promptly notifying the Privacy Officer in the event of any confidentiality incident or other loss or theft of, unauthorized access to, or use or disclosure of personal information, or any other breach in the protection of personal information.

Recommended security measures

To prevent against loss, theft, unauthorized access, use, or disclosure of personal information, or any other breach in the protection of personal information the CIOC recommends the following security measures:

- Keeping physical records organized in locked filing cabinets.
- Avoiding leaving sensitive personal information out in the open, such as on desks.
- Placing digitally stored information behind password protection according to the sensitivity of the information, limiting access to authorized individuals.
- Installing reputable anti-virus software on all company computers and other devices, and asking all employees who use personal devices for work purposes to install anti-virus software on their devices using the CIOC's subscription.
- Ensuring that platforms and computers storing personal information implement strong, randomly generated passwords and two-factor authentication whenever possible.

- Avoiding
  sending personal information, especially sensitive personal information, via email, unless email is encrypted and password protected.
- Training employees in cybersecurity best practices.

Failure to comply with this policy

CIOC could face significant fines and/or penalties if it fails to adequately and timely comply with its obligations regarding the processing of personal information. Therefore, any employee who does not comply with this policy may be subject to disciplinary action up to and including termination. Any employee who becomes aware of a violation of this policy shall promptly report any such violation to the Privacy Officer. If you are unsure about any of the requirements in this policy, please contact the Privacy Officer.

Changes to this policy

The CIOC will update this policy at our discretion in consultation with the Privacy Officer when it is determined that a change needs to be made to keep up with best practices, or when changes to applicable Canadian data protection laws or other relevant developments, taking into account new practices or recommendations issued by the Privacy Officer and/or external guidance issued by Privacy Commissioners require us to do so. CIOC employees will be notified in writing of any changes made to this policy, and up-to-date versions will always be available on the CIOC website.

This policy was last updated on June 15, 2023.