

Cultural Human Resources Council (CHRC)

**Personal Information
Protection and
Electronic Documents Act (PIPEDA)
Privacy Policy**

September 2004

1.0 INTRODUCTION.....	3
2.0 CHRC POLICY STATEMENT	3
3.0 PRIVACY OFFICE WITHIN CHRC.....	4
4.0 WHAT IS PERSONAL INFORMATION?	4
5.0 PERSONAL INFORMATION COLLECTED BY CHRC	5
6.0 GENERAL SAFEGUARDS TO PROTECT PERSONAL INFORMATION.....	5
7.0 PROCESS FOR HANDLING REQUESTS FOR PERSONAL INFORMATION.....	6
8.0 REMOVAL OF PERSONAL INFORMATION	7
9.0 PROCESS FOR DESTRUCTION OF PERSONAL INFORMATION	7
10.0 COMPLIANCE CHALLENGES.....	8
11.0 PROCESS FOR HANDLING COMPLIANCE CHALLENGES	8
12.0 REVIEW AND ASSESSMENT	8

1.0 Introduction

This document constitutes the policy and procedures for the protection of personal information as required by Bill C-6, Protection of Personal Information and Electronic Documents Act (hereinafter referred to as “the Act”) for the Cultural Human Resources Council (CHRC)

2.0 CHRC Policy Statement

The statement in italics below is the CHRC policy statement. It has been reviewed and approved by the CHRC Board of Directors and is posted to the CHRC website.

*The Cultural Human Resources Council (CHRC) is committed to protecting any of your personal information in our possession. We will not disclose any of your personal information other than for its intended use, which is “to **strengthen the Canadian cultural workforce by providing leadership and innovative solutions to human resources issues and to better the HR environment within the cultural sector**” (CHRC’s Mission Statement).*

We will only use any personal information for the identified purposes related to this mission, and we will not disclose to others or use this information for other purposes without first obtaining consent from you.

We will work to ensure that any third parties that we do business with are compliant with Personal Information Protection and Electronic Documents Act (PIPEDA) or the territorial or provincial equivalent legislation.

CHRC protects your electronic and paper based data with security systems to prevent unauthorized access, disclosure or misuse.

If you would like to access your personal information please make your request in writing to the contact listed below.

*Title: Executive Director, CHRC
Address: 17 York Street, Suite 201
Telephone Number: (613) 562-1535
Fax Number: (613) 562-2982
Email: info@culturhrc.ca*

3.0 Privacy Office within CHRC

The staff person responsible within CHRC for the protection of all personal information is the Finance Officer who is the designated Privacy Officer in accordance with the Act.

The Privacy Officer, with the assistance of CHRC's Executive Director and Membership Coordinator, will ensure that the CHRC office is compliant with the ten principles contained in the Act that organizations must follow.

The Executive Director of CHRC is ultimately accountable for the compliance with the provisions of the Act. It is his/her responsibility to:

- Maintain this document in a current state;
- Develop and maintain staff training programs and materials concerning these policies and practices; and
- Ensure that CHRC policies and procedures are compliant with the Act.

4.0 What is Personal Information?

Personal information includes any information about an identifiable individual. For example, name, address, gender, age, ID numbers, income, ethnic origin, employee files, opinions, evaluations, comments, social status, or disciplinary actions, existence of a dispute, intentions (for example, to change jobs). An individual's name need not be attached to the information in order for it to qualify as personal information.

Personal information as defined in the Act does not include a member's or an employee's name, title, business address or telephone number or the use or disclosure of personal information strictly for personal purposes, (e.g. personal greeting card list).

5.0 Personal Information Collected by CHRC

The following is a list of personal information collected by CHRC

- Contact lists for information sharing and communications
- Information related to employment at CHRC
- Information received from persons seeking employment at CHRC
- Information received from persons applying for membership with CHRC
- Information received from and about persons registered in workshops, seminars, and other programs offered by the CHRC and/or its partners
- Information received from persons completing comment forms from CHRC workshops, seminars, and other programs offered by the CHRC and/or its partners
- Information posted to the CHRC web site, including the members only section
- Information received from participants in industry consultation activities
- Information provided to and received from third parties, such as consultants, who are contracted by CHRC to do work for CHRC and on behalf of CHRC members

6.0 General Safeguards to Protect Personal Information

To protect the personal information within the CHRC office, the following procedures are in place:

- Main access doors are locked at all times.
- Doors to the accounting office (and files) and the office where the computer servers are located are locked when staff are not in the office.
- The CHRC network uses a combination of hardware, software applications and security polices to secure the CHRC electronic network. The CHRC office has in place an Internet firewall, which has a number of features that are designed to block-unauthorized access to the CHRC network.
- To ensure that our firewall remains secure no CHRC computers are allowed to run any programs that open ports in the firewall that can then be accessed by a hacking program.

-
- All servers and workstations receive regular software upgrades and security patches the installation of which are recommended by our computer vendors
 - A layered Anti-Virus system scans incoming and outgoing e-mails for computer viruses.

7.0 Process for Handling Requests for Personal Information

This process is related to access of information: “A person may request information about the existence, source, use and disclosure (including third parties) of his/her personal information.” The following is the process for handling requests for personal information:

- The person must make a written request to CHRC’s Executive Director for details about his/her personal information
- This request is directed to the Privacy Officer
- The Privacy Officer responds to the person in writing within two weeks of receiving the request
- If the person wishes to obtain a list of personal information on file with CHRC, the Privacy Officer will send him/her a hard copy of the list through the mail, marked confidential
- If an individual would like to personally examine the personal information on file with CHRC, the Privacy Officer will schedule a meeting with that person to give them access to this personal information
- In the letter and/or during the meeting, the Privacy Officer will advise the individual that he/she may follow up at any time
- After sending the letter or holding the meeting with the person, the Privacy Officer will record the letter/meeting information in a hard copy file that is stored in a locked file cabinet

8.0 Removal of Personal Information

A CHRC member, employee, or person on a CHRC contact list may request the removal of the information in Section 4 at any time, subject to legal or contractual restrictions. The request must be made in writing with reasonable notice. If the consent to hold information is withdrawn, CHRC will destroy that information in accordance with the procedures in section 9.0 and carry out any other action related to the implications as necessary.

9.0 Process for Destruction of Personal Information

There are 2 situations when the destruction of personal information will be necessary. This destruction of personal information will occur when there is a withdrawal of the consent of the relevant individual or when the retention of information is no longer necessary in the opinion of CHRC.

The process is as follows for removal of personal information:

- The person requests in writing stating that he/she would like CHRC to remove his/her personal information
- The Privacy Officer will gather the information to be destroyed (in both paper format and electronic)
- The paper-based information will be shredded, then disposed of in either the trash or recycle bin
- The electronic information will be deleted from all of the electronic files where it is stored
- The Privacy Officer will check all of the available electronic drives and files to ensure it is deleted
- The information will be deleted from all backup records on the CHRC server
- Once the information is destroyed, the Privacy Officer will record the following information and keep it in a labeled destruction of personal information file

-
- The file will be stored in a locked file cabinet, only accessible by the Executive Director and the Privacy Officer

10.0 Compliance Challenges

Any individual may address a challenge concerning CHRC compliance with the Act with respect to section 4.0 to the Privacy Officer. The complaint procedure is outlined in section 11.0. CHRC will investigate all complaints, and if justified, take appropriate measures, including amending these policies and procedures.

11.0 Process for Handling Compliance Challenges

When CHRC receives a compliance challenge or complaint, the following steps will be taken:

- When the challenge or complaint is received in the CHRC office, the Privacy Officer is immediately made aware of the information received including the contact information for the complainant
- When the challenge or complaint is communicated orally, the person will be asked to complete the request in writing and return it to the Privacy Officer
- When the Privacy Officer receives the request in writing, the Privacy Officer reviews it and responds to the petitioner within a reasonable amount of time

12.0 Review and Assessment

This PIPEDA policy and contents will be assessed, reviewed and updated on at least an annual basis or more frequently as amendments to the Act necessitate. As the contents of this policy are dynamic, each CHRC staff member will be required to review this policy once a year, to maintain their knowledge of privacy requirements and provide feedback on the content.