Central Plains

Privacy Policies & Procedures

Created: February 1, 2019

Privacy Management Program Code

Effective Date: February 1, 2019
Reviewed & Created by FCL: October 15, 2018 (cancels September 8, 2015 policy)
Issued By: Strategy Business Unit
Applies To: Retails in the Co-operative Retailing System

INTRODUCTION

Canadian federal and provincial laws require that Central Plains Co-operative Ltd. ("Co-op") maintain the accuracy, confidentiality, and security of personal information collected, used and retained by Co-op. These laws also require Co-op to limit the use of personal information collected by Co-op to the stated purposes for which it was collected and to retain personal information only for as long as required for those purposes or as long as is required to fulfill Co-op's other legal obligations. In addition, Co-op may have contractual obligations to maintain the confidentiality and security of information entrusted to Co-op and to limit use of that information.

The *Co-op Privacy Management Program Code* ("Co-op Privacy Code") is a formal statement of principles and privacy management program guidelines for the protection of personal information collected, used and retained by Co-op. The Co-op Privacy Code outlines the responsibilities of Co-op and its employees for adherence to applicable privacy laws and the related privacy policies and practices of Co-op.

The Co-op will comply with privacy laws within each jurisdiction in which it operates. Sometimes the privacy laws and/or an individual's right to privacy may vary from one jurisdiction to another. The Co-op Privacy Code was developed to treat Co-op employees and customers as consistently as possible. Specific privacy practices may be adopted to address the specific privacy requirements of a particular jurisdiction.

The Co-op Privacy Code explains the obligations of Co-op employees in assisting Co-op in collecting, using, disclosing and maintaining the security of personal information. In addition, Co-op Privacy Code provides Co-op employees with information on the purposes for which the personal information of Co-op's employees is collected, used, retained and disclosed.

SUMMARY OF PRINCIPLES

Principle 1 - Accountability

Co-op is responsible for personal information under its control and has designated a person who has overall accountability for compliance with the following principles. However, each employee of Co-op is responsible for following the Co-op Privacy Code and assisting Co-op in complying with applicable laws.

Principle 2 - Identifying Purposes for Collection of Personal Information

Co-op identifies the purposes for which personal information is collected at or before the time the information is collected. Co-op employees who collect personal information on behalf of Co-op must be prepared to explain the purposes for collection.

Principle 3 - Obtaining Consent for Collection, Use or Disclosure of Personal Information
Meaningful, express consent (or, where reasonable, meaningful implied consent) of a customer or employee is required for the collection, use or disclosure of personal information, unless a legal exception applies.

Principle 4 - Limiting Collection of Personal Information
Personal information is collected only if it is necessary to achieve the purposes identified to the individual.

Principle 5 - Limiting Use, Disclosure and Retention of Personal Information
The fact that Co-op has personal information of a customer does not mean that the personal information can be used for any purpose, disclosed for any purpose or retained indefinitely. When employees use personal information, they should consider whether the use was one that was identified to the person from whom the information was collected. Personal information should not be disclosed without consent unless required by law. Personal information should not be retained for longer than is necessary to fulfill the purpose and to comply with regulatory requirements or to protect Co-op's legal right

Principle 6 - Accuracy of Personal Information
Co-op employees should take care to keep personal information that they are responsible for maintaining as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.

Principle 7 - Security Safeguards
Co-op uses administrative procedures, technical controls and physical security safeguards to protect personal information. Co-op employees must never circumvent or attempt to circumvent these safeguards. If a Co-op employee believes that there is a security breach, or the safeguards are not being complied with, that employee must report the issue to his or her supervisor or, if necessary, to the Chief Privacy Officer.

Principle 8 - Openness Concerning Policies and Practices
The Co-op makes available to customers and employees specific information about its policies and practices relating to the management of personal information.

Principle 9 - Customer and Employee Access to Personal Information
Upon request, Co-op will inform a customer or employee of the existence, use and disclosure of his or her personal information and shall give the individual access to that information. A Co-op customer or employee shall be able to challenge the accuracy and completeness of the information and to have it amended as appropriate.

Principle 10 - Challenging Compliance
Co-op employees should be able to direct any person who wishes to challenge Co-op's compliance with this Privacy Code to the Chief Privacy Officer.

SCOPE AND APPLICATION
The scope and application of Co-op Privacy Code are as follows:

- The Co-op Privacy Code applies to personal information about customers and employees of Co-op that is collected, used or disclosed by it.

- The Co-op Privacy Code applies to the management of personal information in any form whether oral, electronic or written.

- The application of Co-op Privacy Code is subject to the requirements or provisions of any applicable legislation, regulations, or agreements, or the order of any court or other lawful authority.

- The Co-op Privacy Code does not apply to an individual's business contact information so long as that business contact information is used to contact an individual in relation to their business responsibilities and for no other purpose.

DEFINITIONS
"Chief Privacy Officer" – means the individual designated by Co-op to oversee compliance with Co-op Privacy Code.

"Collection" – means the act of gathering, acquiring, recording or obtaining personal information from any source (including third parties) by any means.

"Consent" – means voluntary agreement to the collection, use and disclosure of personal information for defined purposes. Consent can be either express or implied and can be provided directly by the individual or by an authorized representative. Express consent can be given orally, electronically or in writing. Implied consent is consent that can reasonably be inferred from an individual's action or inaction in the circumstances. Consent of an individual is only valid if it is reasonable to expect that the individual understands the nature, purpose and consequences of the collection, use or disclosure of personal information to which they are consenting.

"Customer" – means an individual (member or non-member) who is not a Co-op employee and who:
(a) purchases, uses, or applies to use, the products or services of Co-op;
(b) communicates with Co-op to ask a question, to make a complaint or to give a compliment;
(c) uses a website or other interactive tool provided by Co-op; or
(d) participates in a promotional marketing program or enters a contest sponsored by Co-op.

"Disclosure" – means making personal information available to a third party for the third party's own use and purposes.

"Employee" – means an employee of Co-op.

"Co-op" – means Central Plains Co-operative Ltd.

"Identified Purposes" – means the purposes identified in Principle 2.

"Personal Information" – means information about an identifiable individual but not aggregated information or de-identified information that cannot be associated with a specific individual.

- For a **customer**, such information includes their credit information, billing records, personal address and telephone number, SIN and other particular information which identifies the individual.
- For an **employee**, such information includes information found in personnel employment files, performance appraisals and medical and benefits information.

"Share" – means making personal information available to Federated Co-operatives Limited or a third party who processes or performs services with respect to that personal information on behalf of Co-op. This is sometimes known as "outsourcing".

"Third Party" - an individual other than the customer or his or her agent or an organization other than Co-op, for example: Federated Co-operatives Limited.

"Use" - the treatment, handling, and management of personal information by Co-op, or by Federated Co-operatives Limited, or by a third party.

THE CO-OP CODE IN DETAIL

Principle 1 - Accountability

The Co-op is responsible for personal information under its control and has designated a person who has overall accountability for compliance with the following principles. However, each Co-op employee is responsible for following Co-op Privacy Code and assisting Co-op in complying with applicable laws.

a) Senior Leadership Team of Co-op, in conjunction with its designates, monitors, audits and enforces the provisions of Co-op Privacy Code. Co-op has designated a Chief Privacy Officer to oversee compliance with Co-op Privacy Code. The Chief Privacy Officer can be contacted at:

Chief Privacy Officer
Gordon Van Kannel, Operations Manager
Level 2 – 117 1st Avenue East, Box 970, Rosetown SK S0L 2V0

Office Phone: (306) 882-2601 Cell Phone: (306) 831-4220 Fax: (306) 882-2210
Email: gvankannel.cpcl@sasktel.net

b) Every Co-op employee is responsible for complying with Co-op Privacy Code.

c) Co-op employees are responsible for personal information in their possession or control during the course of their duties, including information that has been shared with a third party for processing. When information is transferred to third parties, Co-op's employees will use appropriate means to provide a comparable level of protection as provided by Co-op Privacy Code. If a Co-op employee requires assistance in determining whether the arrangements with a third party are comparable, the Co-op

employee should contact the Chief Privacy Officer.

d) Individuals and organizations that deal with Co-op have the right to know who is accountable for Co- op's privacy practices. In addition, individuals have the right to access their personal information. Co-op employees will make known to an individual with a privacy inquiry the name and contact information for the Chief Privacy Officer. If a Co-op employee receives a request for information about Co-op's privacy practices that the Co-op employee cannot answer or if a Co-op employee receives a request for access, the Co-op employee should notify the Chief Privacy Officer.

e) Co-op has implemented policies and procedures to give effect to Co-op Privacy Code, including:
   A. implementing procedures to protect personal information and to oversee the company's compliance with Co-op Privacy Code;
   B. establishing procedures to receive and respond to inquiries or complaints;
   C. training and communicating to employees about Co-op's policies and practices; and
   D. developing public information to explain Co-op's policies and practices.

Principle 2 - Identifying Purposes for Collection of Personal Information

Co-op identifies the purposes for which personal information is collected at or before the time the information is collected. Co-op employees who collect personal information on behalf of Co-op must be prepared to explain the purposes for collection.

a) The Co-op collects personal information from its employees for the purposes of establishing, managing or terminating employment relationships. These purposes include:
   A. determining eligibility for initial employment, including the verification of references and qualifications;
   B. assessing qualifications for a particular job or task;
   C. administering pay and benefits;
   D. establishing a contact point in the event of an emergency (such as next of kin);

E. compiling company directories;
F. ensuring the security of company-held information;
G. complying with applicable labour or employment obligations;
H. processing employee work-related claims (e.g. worker's compensation, insurance claims, etc.);
I. establishing training, performance and/or development requirements;
J. conducting performance reviews and providing constructive feedback;
K. engaging in progressive discipline or termination of employment; and
L. for any additional purposes that Co-op advises an employee of and for which Co-op either (a) receives an employee's express or implied consent or (b) is permitted to collect information by law. Co-op may advise an employee of these purposes orally or through written policies. Co-op written policies include (without limitation) the Social Media Policy (ROM 10.00.04), and the Internet and Email Policy (ROM 719.00.01)

b) The Co-op collects personal information from members, customers, vendors, and contractors for the purposes of developing, establishing and maintaining responsible commercial relations. These purposes include:

A. understanding customer preferences and needs;
B. marketing existing and new products and services;
C. increasing brand awareness and loyalty;
D. managing and developing business operations;
E. complying with legal and regulatory requirements;
F. collecting receivables, enforcing legal rights and defending Co-op in litigation;
G. securing and protecting Co-op's property interests, including intellectual property;
H. protecting Co-op employees;
I. for any additional purposes that Co-op advises customers of and either (a) Co-op receives their express or implied consent or (b) Co-op is permitted to collect information by law.

c) Where applicable, Co-op collects information regarding the use of its websites and social media sites for the purposes of developing its brand and relationships with customers and potential customers, potential employees, and managing its information technology and social media assets. These purposes include:

A. to process requests, such as providing members and customers with information and updates that they request;
B. to permit users of social media sites to post a review;
C. to prepopulate information in forms so that users of Co-op's websites do not need to enter it more than once;
D. to help members and customers find information and services;
E. to research and test improvements to Co-op's marketing and promotional efforts and to Co-op's website, including the content and layout of Co-op's websites; and
F. to understand the general marketplace and the interests of visitors to Co-op's websites and social media sites;

G. to monitor and preserve the integrity and security of Co-op's websites, such as to monitor traffic, to administer Co-op's systems, to troubleshoot problems, and to detect attempts at unauthorized access or modification of Co-op's websites or systems.

d) Subject to certain exceptions, personal information may only be used for those identified purposes for which it was collected and for which Co-op has the expressed or implied consent of the individual to whom the personal information relates. The exceptions are discussed under Principle 5.

e) Before collecting personal information, Co-op employees must specify the identified purposes for which the personal information is collected. Co-op employees must, upon request, explain the identified purposes or refer the requester to a designated person within Co-op or the Chief Privacy Officer who will explain or assist in explaining the identified purposes.

f) When explaining or describing the identified purposes, Co-op employees should be as specific as possible. However, Co-op employees should also consider whether there are any future purposes for which Co-op may require the personal information. Unless permitted by law, Co-op may not be able to use or disclose, for any new purpose, personal information that has been collected without first identifying and documenting the new purpose and obtaining the consent of the individual.

g) If a Co-op employee is in doubt about the proper explanation or description of an identified purpose or whether there are future purposes not captured in the explanation or description being used by Co-op, the Co-op employee should raise the issue with his or her supervisor or the Chief Privacy Officer.

Principle 3 - Obtaining Consent for Collection, Use or Disclosure of Personal Information
Meaningful, express consent (or, where reasonable, meaningful implied consent) of a customer or employee are required for the collection, use or disclosure of personal information, unless a legal exception applies.

a) Meaningful consent requires that Co-op employees disclose information regarding the identified purposes (see Principle 2) and provide the individual providing the personal information with an opportunity to make a choice as to whether or not to provide the personal information to Co-op.

b) Before obtaining consent to the collection of personal information, Co-op employees should advise the individual of the identified purposes for which personal information will be used or disclosed. Co-op employees should state the purposes in a manner that can be reasonably understood by the individual.

c) The Co-op may not require customers to consent to the collection, use or disclosure of personal information as a condition of the supply of a product or service, unless such collection, use or disclosure is required to fulfill the identified purposes. For example:
   A. The Co-op may not require a customer to agree to be added to an email marketing promotion as a condition of being a Co-op customer.

B. However, Co-op may require a customer to provide personal information to verify their identity when contacting Co-op in relation to their account.

d) Co-op employees should not develop content (including scripts and software) or design websites, social media pages/channels/sections or sites, or online advertising in ways that collect information or install tracking cookies or other online tracking technologies without the consent of users and without the involvement of the Chief Privacy Officer. When entering into contracts with third parties for website and online marketing, Co-op employees should ensure that third parties disclose all online tracking technologies that will be used to gather information on Co-op's behalf or on Co-op's websites and social media sites. Tracking must be approved by and is subject to review by Co-op.

e) Sometimes it will not be possible or practical to obtain consent to all of the proposed uses of personal information before collection. It is not acceptable to use vague language to obtain consent to future unknown and unspecified purposes. Instead, Co-op will seek new consent to use and disclose personal information for the new purpose once that purpose is known.

f) In general, Co-op will seek to obtain express consent to the identified purposes. However, in some circumstances, it will be reasonable for Co-op to rely on implied consent. For example:

A. If a customer emails Co-op with a question, Co-op may rely on implied consent to use the customer's email address or other contact information in the email to respond to the question. However, Co-op may not add the customer to an email newsletter list or enter the customer in a promotion without the customer's express consent.

B. If an individual accepts employment at Co-op, Co-op may rely on implied consent to use the individual's personal information for payroll and other employment purposes. However, Co-op may not provide employment information to the individual's bank or credit union without the employee's express consent.

C. If a Co-op employee is a member of a public social network (such as Facebook), Co-op may rely on implied consent to monitor the Co-op employee's compliance with Co-op's Social Media Policy (ROM 10.00.04) in posts made publicly.

D. If a former Co-op employee refers a prospective employer to Co-op for a reference, Co-op may rely on implied consent to disclose personal information relating to the former Co-op employee's employment history and competencies.

g) Consent to collect, use and disclose sensitive personal information is done with express consent.

A. Sensitive personal information includes information that could be used for identity theft purposes such as a person's Social Insurance Number, driver's licence number, health card number, and credit card number or other financial information.

B. Sensitive personal information also includes information that could be used or could be perceived to be used to discriminate against a person, such as race, ancestry, place of origin, colour, ethnic

origin, citizenship, creed, sex, sexual orientation, gender identity, gender expression, age, marital status, family status or disability.

C. Co-op employees must not collect personal information from a credit or consumer reporting agency (a credit check) without obtaining the express consent of the person who is the subject of the credit check.

h) In certain circumstances personal information can be collected, used or disclosed without the knowledge and consent of the individual. See Principle 5 for details.

i) A Co-op customer or employee may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. Co-op customers and employees may contact Co-op for more information regarding the implications of withdrawing consent.

Principle 4 - Limiting Collection of Personal Information

Personal information is collected only if it is necessary to achieve the purposes identified to the individual.

a) Where feasible, Co-op employees should assess the privacy implications of new corporate and sales initiatives before implementing them to ensure that only personal information that is necessary to fulfill the purpose of the initiative is collected and that the means that are proposed to be used to obtain consent are adequate. For example:

A. The precise date of birth is rarely required for a contest or promotion. The contestant may be asked instead to confirm that he or she is of the age of majority.

B. Requiring a Social Insurance Number from all applicants for a job (prior to any offer being made) may not be required and may lead to allegations of discrimination, since it may be possible to tell whether the applicant is a citizen or permanent resident or a temporary worker. The applicant

may be asked instead to confirm eligibility to work in Canada.

b) Co-op employees should collect personal information in a transparent way. Whenever possible, Co-op employees should collect personal information directly from the person regarding whom the personal information relates.

c) Co-op may also collect personal information from other sources including credit bureaus, former employers or personal references, or other third parties that represent that they have the right to disclose the information. This information should only be collected where it is necessary and where the possibility of this collection has been disclosed.

Principle 5 - Limiting Use, Disclosure and Retention of Personal Information

The fact that Co-op has personal information of a customer does not mean that the personal information can be used for any purpose, disclosed for any purpose or retained indefinitely. When Co-op employees use

personal information, they should consider whether the use was one that was identified to the person from whom the information was collected. Personal information should not be disclosed without consent unless required by law. Personal information should not be retained for longer than is necessary to fulfill the purpose and to comply with regulatory requirements or to protect Co-op's legal rights.

a) Co-op employees are responsible for ensuring that Co-op complies with its obligations relating to personal information throughout the lifecycle of that information.

b) Co-op's responsibilities begin at the point of collection and remain in place until secure destruction. Co-op's responsibilities do not end when information is transferred to third parties.

c) Co-op employees may share information for identified purposes with third parties who process or perform services with respect to that personal information on behalf of Co-op. For example:
   A. Co-op may share an employee's personal information with a benefits service provider for the purpose of the administration of employee benefits.
   B. Co-op may share customer email addresses with a marketing service provider for the purposes of providing customers with email newsletters.
   C. Co-op may retain a third party to host servers and software programs in which employee and customer personal information is stored and processed.

d) Third parties with whom Co-op shares personal information may be located in the United States of America or in other locations around the world. Co-op is responsible for ensuring that personal information transferred to third parties is subject to comparable levels of security protection as in Canada. However, personal information that is stored or used in another jurisdiction will be subject to the laws of that jurisdiction, which may not afford the same protections as the laws of Canada. Laws and regulations in the United States (and other countries) may require disclosure of such information to the United States government or its agencies in certain circumstances.

e) Before Co-op shares personal information with a third party, Co-op employees should consider the

   administrative, technical and physical security precautions in place to prevent unauthorized access, use or disclosure of the personal information while the information is transferred to and used by the affiliate or third party. For example:
   A. Co-op employees should not email a spreadsheet of highly sensitive personal information, such as banking information, unless the email or spreadsheet is encrypted.
   B. Co-op employees should ensure that third parties only receive personal information that is necessary to perform the service for Co-op. The third party should be required to maintain the security of the personal information at all times.

f) Third parties may not use information shared by Co-op for purposes other than identified purposes unless

consent is obtained from the individual whose personal information is being used for a new purpose. See Principles 2 and 3.

g) Only those Co-op employees who require access for business reasons or whose duties reasonably so require are granted access to personal information about Co-op members, customers and employees.

h) Unless Co-op has issued a hold on destruction of records (sometimes called a "legal hold" or "litigation hold") in order to comply with its obligations to retain records that may be relevant to a legal risk, Co-op employees must comply with Co-op record retention and information classification policies to ensure that personal information is not retained for unreasonable periods of time.

   A. In general, personal information should only be kept as long as it is necessary for the identified purposes.

   B. In certain cases, personal information may be required to be maintained for longer periods of time in accordance with other laws. For example, records relevant to product safety, employment decisions, or Co-op's responsibilities under import/export or taxation legislation may be required to be kept for significant periods of time. In addition, Co-op will require employees to suspend record destruction processes for records that may be relevant to actual or anticipated litigation.

   C. Co-op employees are required to comply with Co-op retention and destruction schedules and procedures. If personal information is to be kept beyond what is necessary to fulfill the identified purposes or to comply with laws regarding the retention of documents, the information must be de- identified and rendered permanently anonymous.

i) Co-op employees should always seek advice from their supervisor or, if appropriate, the Chief Privacy Officer, before disclosing personal information to a third party without the consent of the individual whose information has been collected.

j) There are rare situations in which Co-op, its affiliates and retail co-op members may use personal information or Co-op may disclose personal information to a third party without the consent of the individual whose information has been collected. For example:

   A. The Co-op may use personal information if Co-op has reasonable grounds to believe that the information would be useful in the investigation of a breach of Canadian, provincial or foreign laws.

   B. The Co-op may use personal information in an emergency that threatens the life, health or security of an individual.

   C. The Co-op may disclose personal information to a lawyer representing the organization in order to obtain legal advice.

   D. The Co-op may disclose personal information for the purpose of collecting a debt owed by the individual to Co-op or in connection with legal proceedings in which Co-op has an obligation to

disclose the personal information. This may include responding to a subpoena or warrant issued or an order made by a Canadian or foreign court with jurisdiction.

E. In certain circumstances, Co-op may disclose personal information to a government institution with lawful authority to request the information for the purposes of enforcing the laws of Canada, a province or a foreign jurisdiction.

Principle 6 - Accuracy of Personal Information

Co-op employees should take care to keep personal information that they are responsible for maintaining as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.

a) The Co-op is responsible for instituting processes to minimize the possibility that inappropriate information may be used to make a decision about a Co-op customer or employee.

b) The Co-op will update personal information about customers and employees as and when necessary to fulfill the identified purposes or upon notification by the individual.

c) The Co-op employees are responsible for following Co-op processes to ensure that personal information is accurate, complete and up-to-date.

Principle 7 - Security Safeguards

The Co-op uses administrative procedures, technical controls and physical security safeguards to protect personal information. Co-op employees must never circumvent or attempt to circumvent these safeguards. If a Co-op employee believes that there is a security breach, or the safeguards are not being complied with, that Co-op employee must report the issue to his or her supervisor or, if necessary, to the Chief Privacy Officer.

a) A Co-op employee who becomes aware of unauthorized access, use or disclosure of personal information should report that unauthorized access, use or disclosure to his or her supervisor and the Chief Privacy Officer. In some cases, Co-op has mandatory breach notification responsibilities, which will be coordinated by the Chief Privacy Officer. See Principle 1.

b) Co-op employees with access to personal information are required as a condition of employment to respect the confidentiality of personal information.

c) Co-op protects personal information against risks such as loss or theft, unauthorized access, disclosure, copying, use, modification or destruction. The methods of protection include:

A. Physical Measures: For example, Co-op employees should not leave documents containing personal information in open areas or on their desk whenever they leave their desk. Documents should be placed in secure locations such as locked cabinets or drawers. Employees should lock their computers whenever they leave their desk. Co-op employees should use security passes to

ensure that access to Co-op offices are restricted to authorized personnel and approved guests. All employees should destroy personal (and other confidential and sensitive) information by means of shredding at designated locations in the building. Employees should ensure that they collect print jobs containing personal (and other confidential and sensitive) information immediately from the printers so that they are not accessed by unauthorized individuals.

B. Organizational Measures: The Co-op restricts access to personal information to a "need-to-know" basis. Co-op employees should not disclose personal information to other employees who do not require access to that information to fulfill their job functions.

C. Technological Measures: Co-op employees are required to use passwords (as per Co-op's password policy) and to keep those passwords secure. Co-op employees should not download personal information to unencrypted devices, such as USB keys, or devices that have not been authorized by Co-op, such as a smart phone. Only authorized and licenced software and hardware is permitted to be connected to Co-op information technology system. The Co-op will take appropriate measures to ensure that the confidential and personal information residing on its computer systems and servers is protected from unauthorized access and encrypted where appropriate. Confidential emails, and those containing personal information, should be encrypted before being sent to recipients. Co-op will take appropriate measures to secure its computer network and electronic resources from unauthorized access by using tools and hardware subject to regular security testing.

d) Co-op employees should ensure that any personal information shared with third parties is protected by contractual agreements stipulating the confidentiality of the information and the purposes for which it is to be used.

Principle 8 - Openness Concerning Policies and Practices

The Co-op makes available to customers, employees and retail co-op members specific information about its policies and practices relating to the management of personal information.

a) Where applicable Co-op maintains a privacy policy on its websites, which describes its privacy practices to retail co-op members and customers.

b) A Co-op employee who has questions or concerns about this Privacy Code or the privacy policy on Co-op websites should discuss his or her questions or concerns with a supervisor or the Chief Privacy Officer. See Principle 1.

c) Individuals have the right to obtain information about Co-op's privacy practices. Individuals also have the right to obtain access to personal information held by Co-op about them. See Principle 9.

d) Co-op has a responsibility to provide information to help customers and employees exercise choices

regarding the use of their personal information and the privacy-enhancing services available from Co-op. Therefore, Co-op employees should:

A. ensure that they are familiar with this Privacy Code;
B. be able to explain Co-op's privacy practices to retail co-op members or customers who make inquiries; and
C. refer questions that Co-op employee cannot answer and any access requests to the Chief Privacy Officer. See Principle 1.

Principle 9 – Customer and Employee Access to Personal Information

Upon request, Co-op will inform a customer or employee of the existence, use and disclosure of his or her personal information and shall give the individual access to that information. A customer or employee shall be able to challenge the accuracy and completeness of the information and to have it amended as appropriate.

a) Co-op is responsible for providing individuals with a reasonable opportunity to review personal information collected about that individual. This includes a description of the type of personal information held by Co-op, including a general account of its use, and the parties to which the personal information has been disclosed.

b) Co-op employees should take care to ensure that access requests are identified and properly processed. Many privacy complaints are related to employees failing to identify and refer access requests to be dealt with in accordance with applicable privacy legislation.

A. A customer can obtain information or seek access to his or her individual file by contacting a designated representative at Co-op's business office.
B. An employee can obtain information or seek access to his or her individual file by contacting Human Resources within Co-op.
C. In all other cases, refer the request to the Chief Privacy Officer. See Principle 1.

c) In certain situations, Co-op may not be able to provide access to all of the personal information that it holds about an individual. For example:

   A. Co-op may not provide access to information if doing so would likely reveal personal information about a third party or could reasonably be expected to threaten the life or security of another individual.

   B. Co-op may not provide access to information if disclosure would reveal confidential commercial information.

   C. Co-op will not provide access if the information is protected by solicitor-client privilege or if the information was generated in the course of a formal dispute resolution process, or if the information was collected in relation to the investigation of a breach of an agreement or a contravention of a federal or provincial law.

d) If access to personal information is not provided, Co-op will provide the reasons for denying access upon request. Copies of Access Denial letters will be maintained on file by the Chief Privacy Officer or designate.

e) In order to safeguard personal information, an individual may be required to provide sufficient identification information to permit Co-op to account for the existence, use and disclosure of personal information and to authorize access to the individual's file. Any such information shall be used only for this purpose.

f) Co-op is responsible for promptly correcting or completing any personal information found to be inaccurate or incomplete. Co-op employees should not refuse or neglect to correct or complete personal information. For example, if a customer requests to be removed from a distribution list, Co-op employees should promptly process or forward the request to the appropriate person for processing.

g) Any unresolved differences as to accuracy or completeness should be noted in the individual's file. In certain circumstances, Co-op will also transmit to third parties having access to the personal information in question any amended information or the existence of any unresolved differences.

Principle 10 - Challenging Compliance

Co-op Employees should be able to direct any person who wishes to challenge Co-op's compliance with this Privacy Code to the Chief Privacy Officer.

a) Co-op maintains procedures for addressing and responding to all inquiries or complaints about Co-op's handling of personal information.

b) If a Co-op employee is not able to answer an inquiry about Co-op's handling of personal information, the Co-op employee should refer the inquiry to the employee's supervisor or the Chief Privacy Officer. See Principle 1.

c) If a Co-op employee receives a complaint, the complaint should be forwarded to the Chief Privacy Officer who may delegate the investigation of the complaint and the response. See Principle 1.

d) In addition, Co-op employees should ensure that they inform customers that they are entitled to complain to the Chief Privacy Officer in the event of a dispute and provide the customer information on how to contact the Chief Privacy Officer. See Principle 1.