PRIVACY POLICY UNDER THE *PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT* (*PIPEDA*) *OF MINOR BAY LODGE & OUTPOSTS LTD. (HEREINAFTER REFERRED TO AS MINOR BAY)*

Date of Privacy Policy January / 1 / 2001

OVERVIEW

The purpose of *PIPEDA* is to establish the rules for organizations to follow in handling personal information. The intention of *PIPEDA* is to balance an individual's right to privacy of his or her personal information with a need for organizations to collect, use or disclose personal information for legitimate business purposes.

PIPEDA applies to all businesses that collect, use or disclose personal information in the course of their commercial activities or is about an employee of an organization that collects, uses or discloses in connection with the operation of a federal work, undertaking or business.

Generally, an organization is required to obtain an individual's consent when they collect, use or disclose that individual's personal information. Personal information can only be used for the purpose that it was collected for and consented to. Consent must be obtained again if the organization intends to use the information for another purpose.

The individual has a right to access his or her personal information that is held by the organization and, if necessary, challenge the accuracy of that information. An organization has an obligation to provide personal information in an alternative format for a person with a sensory disability. Examples of alternative formats include audio tape, Braille or large print.

An organization must assure individuals that proper safeguards are in place to keep the personal information safe. Examples of specific safeguards would include: encrypting electronic documents, securing computer use by controlling computer passwords and keeping all physical versions of personal information in locked filing cabinets.

OFFENCES

Offences under *PIPEDA* include:

- a person destroying personal information that has been requested by an individual;
- an employer demoting, disciplining, dismissing, harassing, suspending or disadvantaging in any way an employee who has complained to the Privacy Commissioner, or who has refused to do anything that is in contravention of protecting personal information as required by *PIPEDA*;
- a person obstructing an audit or an investigation into a complaint investigation that is being conducted by the Privacy Commissioner or his delegate.

Liability for a summary offence carries a maximum $10,000 fine. Liability for an indictable offence carries a maximum $100,000 fine.

DEFINITIONS

Commercial activity

Commercial activity means any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists.

Consent

Consent is the voluntary agreement with what is being done or proposed. Consent can be either express or implied. Express consent is given explicitly, either orally or in writing. Express consent is unequivocal and does not require any inference on the part of the organization seeking consent. Implied consent arises where consent may reasonably be inferred from the action or inaction of the individual.

Disclosure

Disclosure is making personal information available to others outside the organization.

Federal work, undertaking or business

Examples of a federal work, undertaking or business include:

- shipping operations;
- railways, canals, telegraphs;
- ferries;
- aerodromes, aircrafts, airlines;
- radio broadcasting stations;
- banks;
- works that are declared by Parliament to be advantageous to two or more provinces or Canada;
- a work, undertaking or business that operates outside exclusive provincial legislative authority.

Organization

Organization includes an association, a partnership, a person and a trade union.

Personal health information

Personal health information with respect to an individual, whether living or deceased, means:

- information concerning the physical or mental health of the individual;
- information concerning any health service provided to the individual;
- information concerning the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;
- information that is collected in the course of providing health services to the individual;
- information that is collected incidentally to the provision of the health services to the individual.

Personal information

Personal information means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization.

Personal information can be factual or subjective information, whether recorded or not, that is about an identifiable individual. Examples of personal information include:

- age, name, ID numbers, income, ethnic origin or blood type;
- opinions, evaluations, comments, social status or disciplinary actions;
- employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions (for example, to acquire goods or services, or change jobs).

Personal information that is not covered by the *Act* includes:

- personal information that is collected, used or disclosed by federal government organizations that are listed under the federal *Privacy Act*, or by provincial or territorial governments and their agents;
- the name, title, business address and telephone number of an employee;
- collection, use or disclosure of information by an individual that is strictly for personal purposes, such as a personal greeting card list;
- collection, use or disclosure of information by an organization that is solely for artistic, journalistic or literary purposes

Use

Use refers to the treatment and handling of personal information within an organization.

PERSONAL INFORMATION PROTECTION POLICY

Generally, all businesses are required to comply with *PIPEDA* and follow the code of principles for protecting personal information that is collected, used and disclosed, such that individuals have control over how their personal information is handled in the private sector. Organizations must ensure that all personal information is handled fairly within their own organization and when that information is disclosed to third parties.

PIPEDA sets out obligatory provisions and recommended provisions for complying with *PIPEDA* and the code of principles. The collection, use and disclosure of personal information must be limited to purposes that a reasonable person would consider appropriate in the circumstances. The perspective of the reasonable person must be considered in applying any provisions of *PIPEDA* that pertain to the collecting of personal information. Organizations must ensure that all personal information is handled fairly within their own organization and when that information is disclosed to third parties.

This policy is set out to ensure that ***Minor Bay*** complies with *PIPEDA* and its ten principles for the fair handling of personal information.

1. ACCOUNTABILITY

Responsibilities

Minor Bay is responsible for:

- complying with the ten principles;
- appointing an individual or individuals to be responsible for the organization complying with *PIPEDA*;
- protecting all personal information that is held by the organization or transferred to third parties for processing; and
- developing and implementing personal information policies and practices.

The Ten Principles

Minor Bay must comply with all ten principles that are set out in Schedule 1 of *PIPEDA* and are:

1. Accountability;
2. Identifying purposes;
3. Consent;
4. Limiting collection;
5. Limiting use, disclosure, and retention;
6. Accuracy;
7. Safeguards;
8. Openness;
9. Individual access;
10. Challenging compliance;

These principles are the basis of the framework that is being used for this policy.

Designated Privacy Officer

The following individual***[s] [is/are]*** appointed to be responsible for the organization's compliance with *PIPEDA: **Darlene Blue***

The designated privacy officer ***has*** the support of senior management in carrying out ***her*** responsibilities to ensure that ***Minor Bay*** complies with *PIPEDA*. The designated privacy officer ***has*** the authority to intervene on any privacy issues that arise in the operation of the organization's business. The designated privacy officer ***is*** responsible for ensuring that the organization complies with *PIPEDA* at all times in the handling of personal information.

The name or title of the designated privacy officers will be communicated internally and externally and will be included, for example, in the organization's publications and on the organization's Web site.

By designating a privacy officer to be accountable for the organization complying with *PIPEDA* does not relieve ***Minor Bay*** from complying with the ten principles.

Protection of personal information within the organization

All personal information handling practices, including ongoing activities and new initiatives, will be analyzed on an ongoing basis to ensure that they comply with fair information practices.

Anyone collecting, using or disclosing personal information on behalf of the organization must be able to answer the following questions. If not, that person must get clarification from the designated privacy officer before proceeding. The questions are:

1. What personal information do we collect?
2. Why do we collect it?
3. How do we collect it?
4. What do we use it for?
5. Where do we keep it?
6. How is it secured?
7. Who has access to or uses it?
8. To whom is it disclosed?
9. When is it disposed of?

The organization is committed to training staff on privacy policies and procedures to ensure that they can answer the following questions:

- How do I respond to public inquiries regarding our organization's privacy policies?
- What is consent? When and how is it to be obtained?
- How do I recognize and process requests for access to personal information? To whom should I refer complaints about privacy matters? What are my privacy protections and rights? (This applies to employees in federally regulated organizations.)
- What are the ongoing activities and new initiatives relating to the protection of personal information at our organization?

Third party guarantee

All third parties must guarantee in writing that they will handle the personal information in compliance with *PIPEDA* and will refer all requests for access to personal information to the organization prior to any personal information being transferred to them.

When transferring personal information to third parties, ensure that a privacy protection clause is included in all contracts to guarantee that the third party provides the same protection of the personal information as does ***Minor Bay***:

- Name a person to handle all privacy aspects of the contract;
- Limit use of the personal information to the purposes specified to fulfil the contract;
- Limit disclosure of the information to what is authorized by your organization or required by law;
- Refer any people looking for access to their personal information to your organization;
- Return or dispose of the transferred information upon completion of the contract;
- Use appropriate security measures to protect the personal information;

- Allow your organization to audit the third party's compliance with the contract as necessary.

Development and implementation of privacy policies and practices

Minor Bay is responsible for developing and implementing personal information policies and practices and has developed and implemented policies and procedures in order to protect personal information in compliance with *PIPEDA*.

Minor Bay is committed to making information readily available to clients and customers on brochures and on Web sites.

The purpose for collecting personal information must be identified before or at the time of collecting the personal information. Where personal information has already been collected and it is to be used or disclosed for a purpose other than the purpose consented to, consent must be obtained for that new purpose.

Consent must be obtained from each individual providing his or her personal information for each purpose.

Collection, use and disclosure must be limited to the purpose for which consent has been obtained.

Personal information must be correct, complete and current.

Security measures must be adequate for the format in which the personal information exists. All electronic documents containing personal information must be encrypted. All hard copy of personal information including paper files, floppy discs, compact discs, zip drives must be secured in a locked filing cabinet. Only qualified personnel shall have access to the filing cabinet key and must sign in and sign out the key and identify the personal information that they are accessing and its purpose. Similarly, only qualified personnel will be given a computer password to access personal information. A log must be kept of who has accessed the personal information, on what date, and for what purpose.

All personal information is subject to a retention and destruction timetable. The retention period is only long enough for a person to access that personal information where it was used in making a decision about the person, as required by law, or other definable necessary time. Destruction must be done in such a way that no unauthorized personnel can access the information.

2. IDENTIFY THE PURPOSE

Responsibilities

Minor Bay is responsible for:

- identifying the purpose (why it is needed and how it will be used) for the collection of personal information either before or at the time of collecting the personal information;
- documenting why the information is collected;
- informing the individual from whom the information is being collected why that information is needed;
- obtaining consent from the individual for any personal information that has already been collected and is to be used for another purpose.

Identifying the purpose

The reasons for collecting personal information must be identified by ***Minor Bay***, either before or at the time that the information is collected.

Examples of purposes include:

- opening an account;
- verifying creditworthiness;
- providing benefits to employees;
- processing a magazine subscription;
- sending out association membership information;
- guaranteeing a travel reservation;
- identifying customer preferences;
- establishing customer eligibility for special offers or discounts.

These responsibilities are fulfilled by the organization by reviewing all personal information in its holdings and ensuring that it has been collected for a specific purpose. The purpose must be limited to what a reasonable person would expect in the circumstances. Notify the individual either orally or verbally of these purposes.

Documenting the purposes

Minor Bay must identify and document the reason why it is necessary that the personal information is being collected and how that information will be used.

Set up a log to record all identified purposes and the consents that have been obtained for those purposes. This log is to be referred to in the event that an individual would like to access his or her personal information.

Informing the Individual

Each individual who is providing personal information must be informed of the reason that his/her personal information is being collected.

The purposes for collecting personal information must be defined as clearly and narrowly as possible so that an individual can understand how his or her personal information will be used or disclosed. An overly broad purpose may not provide the individual with the appropriate knowledge to give an informed consent.

Obtaining Consent for a New Purpose

Minor Bay must identify any new use of the personal information and obtain consent from the individual before using the information.

3. OBTAIN CONSENT

Responsibilities

The organization is responsible for:

- informing individuals in a meaningful way as to the purpose that his or her personal information is to be collected, used or disclosed; and

- obtaining consent before or at the time of collecting the personal information and obtaining consent for any new purposes after the information has been collected but before that information is used or disclosed for the new purpose.

Informing individuals

The organization must ensure that the individual is properly informed as to the purpose that his or her personal information is to be collected, used or disclosed. The organization must ensure that consent is obtained for every new purpose prior to implementing the new use for the personal information.

Ensure that consent is obtained every time personal information is collected, used or disclosed. Ensure that the purpose for collecting the personal information is communicated in a clear and reasonably understandable manner. Record details of consent, if it was received verbally. File the consent itself, if in writing. For example, where the consent is verbal, a note is made to the file. Where consent is made by e-mail, a copy of the e-mail is included in the file. Where consent is given by checking off a box, a copy of that checked off consent should be included in the file. The organization must ensure that no one obtains consent by deceptive means as this method does not meet the requirement of informed consent.

Consent to collect, use or disclose a customer's personal information must not be conditional on the supplying of a product or a service, unless the requested personal information is necessary in order to fulfil an explicitly specified and legitimate purpose. Individuals must be informed of the implications of withdrawing their consent. The organization must ensure that employees who are collecting personal information are able to answer an individual's questions about why the employee is collecting the information.

Consent is usually collected from the person who is the subject of the personal information that is collected, used or disclosed.

Consent may be obtained from a legal guardian where the individual is a minor, or a person having power of attorney for a person who is seriously ill or mentally incapacitated. Consent is only meaningful if the individual understands how his or her information is going to be used or disclosed.

Consent clauses should:

- be easy to find;
- use clear and straightforward language;
- not use blanket categories for purposes, uses or disclosures;
- be specific as possible about which organizations handle the personal information.

Consent can be obtained in person, over the telephone, by mail or over the Internet. The form of consent should relate to:

- the reasonable expectations of the individual;
- the circumstances surrounding the collection;
- the sensitivity of the information involved.

Whenever possible, express consent is the best form of consent, however, express consent should always be used when collecting or disclosing personal information that is considered sensitive. Express consent provides protection for both the individual and the organization.

Obtaining consent for any new purpose

Any new purposes for the use or disclosure of personal information must be documented. The same procedures for obtaining consent in the first instance apply to obtaining consent for new purposes, including:

- informing the individual of the new purpose for information that has already been collected;
- documenting the consent.

Grandfathering provisions

All personal information that has been collected by the organization during the course of its commercial life is subject to *PIPEDA*. This information does not need to be recollected, however, consent to use or disclose this information upon the implementation of *PIPEDA* (generally, January 1, 2004 for private-sector businesses) is required. ***Minor Bay will inform*** its clients and customers what the organization does with the personal information, to whom the organization discloses that personal information, and ***will give*** them the option of the ongoing uses or disclosures of their personal information.

Exceptions to consent

Personal information can only be collected by ***Minor Bay*** without the individual's knowledge or consent:

- if it is clearly in the individual's interests and consent is not available in a timely way;
- if knowledge and consent would compromise the availability or accuracy of the information and collection is required to investigate a breach of an agreement or contravention of a federal or provincial law;
- for journalistic, artistic or literary purposes;
- if it is publicly available as specified in the regulations.

Personal information can only be used by ***Minor Bay*** with the individual's knowledge or consent:

- if ***Minor Bay*** has reasonable grounds to believe the information could be useful when investigating a contravention of a federal, provincial or foreign law and the information is used for that investigation;
- for an emergency that threatens an individual's life, health or security;
- for statistical or scholarly study or research (***Minor Bay*** must notify the Privacy Commissioner before using the information);
- if it is publicly available as specified in regulations;
- if the use is clearly in the individual's interest and consent is not available in a timely way;

- if knowledge and consent would compromise the availability or accuracy of the information and collection was required to investigate a breach of an agreement or contravention of a federal or provincial law.

Personal information can only be disclosed by ***Minor Bay*** with the individual's knowledge or consent:

- to a lawyer representing ***Minor Bay***;
- to collect a debt the individual owes to ***Minor Bay***;
- to comply with a subpoena, a warrant or an order made by a court or other body with appropriate jurisdiction;
- to a government institution that has requested the information, identified its lawful authority, and indicates that disclosure is for the purpose of;
    - enforcing, carrying out an investigation, or gathering intelligence relating to any federal, provincial or foreign law, or
    - suspects that the information relates to national security or the conduct of international affairs, or
    - is for the purpose of administering any federal or provincial law
- the information relates to national security or the conduct of international affairs if made by an investigative body for the purposes related to the investigation of a breach of an agreement or a contravention of a federal or provincial law in an emergency threatening an individual's life, health, or security (***Minor Bay*** must inform the individual of the disclosure);
- for statistical, scholarly study or research (***Minor Bay*** must notify the Privacy Commissioner before disclosing the information);
- to an archival institution;
- 20 years after the individual's death or 100 years after the record was created;
- if it is publicly available as specified in the regulations
- if required by law.

4. LIMIT COLLECTION

Responsibilities

Minor Bay is responsible:

- to not collect information indiscriminately, and
- to not collect personal information by deceptive or misleading means.

No indiscriminate collection or collection by deceptive means

Minor Bay must ensure that personal information is not collected indiscriminately, nor may personal information be collected by deceiving or misleading individuals about why the organization is collecting the information.

Limiting collection

Minor Bay must ensure that the amount and type of information is limited to what is necessary for the identified purposes.

The kind of personal information that ***Minor Bay*** collects is identified in all of our information-handling policies and practices.

Minor Bay will hold staff meetings on a regular basis to ensure that employees can explain to an individual why the personal information is needed.

Minor Bay is committed to reducing the amount of information that is collected in order to lower the cost of collecting, storing, retaining and archiving data. ***Minor Bay*** is also committed to reducing the amount of information that is collected in order to reduce the risk of inappropriate uses or disclosures.

5. LIMIT USE, DISCLOSURE AND RETENTION

Responsibilities

Minor Bay is responsible:

- to ensure that personal information is only used or disclosed for the purpose that the personal information was collected unless the individual consents to another purpose, or the use or disclosure is authorized by *PIPEDA*;
- to ensure that personal information is only kept for as long as is necessary to satisfy the purposes;
- for putting guidelines and procedures in place for the retention and destruction of personal information;
- to keep personal information that has been used to make a decision about a person for a reasonable period of time so that that person can access the information and seek redress, if need be; and
- to destroy, erase or render anonymous information that is no longer needed for an identified purpose or for legal reasons.

Limiting use or disclosure of personal information to the consented purposes

The collection, use and disclosure of personal information must be limited to purposes that a reasonable person would consider appropriate in the circumstances. The perspective of the reasonable person must be considered in applying any provisions of *PIPEDA* that pertain to the collecting of personal information.

Keeping personal information only for as long as is necessary

Personal information is only to be kept as long as is necessary to satisfy the limited purposes. For example, personal information that was used to make a decision concerning a person should be kept for a reasonable time in order to allow the person the ability to obtain the information after the decision is made and pursue whatever options or recourses may be available to that person. Reviews are to be conducted on a regular basis in order to decide whether information is still required and document these decisions on a retention schedule.

6. BE ACCURATE

Responsibilities

Minor Bay is responsible for:

- keeping personal information as accurate, complete and current as necessary in light of its use and interests of the individual;
- updating personal information only when necessary to fulfil the specific purposes;
- keeping frequently used information current and accurate unless limits are clearly set out, or where out-of-date or incomplete information would harm the individual.

7. USE APPROPRIATE SAFEGUARDS

Responsibilities

Minor Bay is responsible for:

- protecting the personal information against loss or theft;
- safeguarding the personal information against unauthorized access, copying, disclosure, modification or use, and;
- protecting the personal information no matter what format the personal information exists in.

Protecting personal information against loss of theft

Minor Bay is committed to ensuring that all employees and any other person handling personal information understands the need to keep personal information confidential and to maintain security measures to protect personal information against loss or theft.

Protecting personal information no matter what the format

Safeguards should be implemented that meet the particular needs of particular formats, such as paper shredding of paper files, and deleting electronic files that contain personal information.

Safeguarding personal information against unauthorized use

In order to protect personal information, the organization has developed and implemented a security policy as follows:

Physical measures

All paper files containing personal information are to be stored in locked filing cabinets at ***Minor Bay's Winnipeg office.*** The key to the locked filing cabinets is only available on a required basis and is documented by and kept with ***Darlene Blue***.

Access to offices that contain personal information are restricted as follows: ***Authorized personnel only***

Electronic measures

Technological tools are to be used to protect all electronic documents:

Passwords and firewalls

Organizational controls

The following factors are to be considered when selecting which safeguards are appropriate for which information:

- sensitivity of the information;
- amount of information;
- extent of distribution;
- format of the information;
- type of storage.

Personal information that is not relevant to a transaction must be concealed or removed prior to providing copies of relevant personal information to others.

Sensitive personal information must be kept in a secure area or computer system and only individuals that "need-to-know" can access these files.

Security measures are to be reviewed and updated on a regular basis to ensure up-to-date training of personnel in light of changes in business practices and advances in technology from time to time.

8. BE OPEN

Responsibilities

Minor Bay is responsible for:

- informing clients, customers and employees that the organization has policies and practices for the management of personal information; and
- making these policies and practices understandable and easily available.

Availability of organization's policies and practices

Information about the organization’s policies and practices are available

On the organization’s web site at http://minorba.ycom.

9. GIVE INDIVIDUALS ACCESS

Responsibilities

Minor Bay is responsible to:

- inform individuals, upon request, if the organization has any information on them, and;
- provide an explanation of how the personal information is or has been used;
- provide a list of organizations to which the personal information has been disclosed;
- provide the individual with access to his or her information;
- amend or correct any personal information if the individual has challenged the accuracy or completeness of the information and it is found to be deficient;

- provide a copy of the requested information or reasons for not providing the requested information.

Any disagreement should be noted on the file and third parties should be advised where appropriate.

The organization will ensure that an individual is given whatever help the individual requires in order to prepare a request. The organization may ask the individual for enough information to enable the organization the account for the existence, use and disclosure of that individual's personal information.

Minor Bay must respond to the request within 30 days of receiving the request. The 30-day period may be extended for an additional maximum 30 days:

- if responding to the request within the original 30 days would unreasonably interfere with activities of your organization;
- if additional time is necessary to conduct consultations;
- if additional time is necessary to convert personal information to an alternate format.

Minor Bay must notify the individual within the initial 30-day period of receiving the request and of the individual's right to complain to the Privacy Commissioner of Canada.

Individuals are to be given access at minimal or no cost. If there is a cost, notify the individual of the approximate costs before the request is processed and he or she is given access to his or her personal information. Ensure the information is understandable. For example, explain acronyms, abbreviations and codes that appear in the information.

In situations where information is amended, send the amended information to any third parties who have access to the information.

Where access is refused, explain in writing the reasons and any available recourse to the individual.

Personal information is kept ***at Minor Bay's Winnipeg office***

Personal information should never to disclosed until the identity of the individual requesting the information has been confirmed as the appropriate individual and that he or she has a right to access that personal information.

Everyone who is handling personal information request must understand the exceptions to providing access.

EXCEPTIONS TO ACCESS

Minor Bay must refuse an individual's access to personal information in the following circumstances:

- if it would reveal personal information about another individual (unless this information can be severed out) unless there is consent or a life-threatening situation;
- if ***Minor Bay*** has disclosed information to a government institution for law enforcement or national security reasons. (In certain situations, a government institution may instruct the organization to refuse access to the individual and/or to not reveal that the information has been released to the government institution. In this situation, the organization must comply with the government institution's request and notify the Privacy Commissioner why the

individual's request was refused. The individual cannot be informed of the disclosure to the government institution, that the institution was notified of the individual's request, nor that the Privacy Commissioner was notified of the organization's refusal of the individual's request.)

Minor Bay must refuse an individual's access to personal information in the following categories:

- solicitor-client privilege;
- confidential commercial information (unless it can be severed out);
- disclosure could harm an individual's life or security (unless it can be severed out);
- it was collected without the individual's knowledge or consent to ensure its availability and accuracy, and the collection was required to investigate a breach of an agreement or contravention of a federal or provincial law (the Privacy Commissioner must be notified);
- it was generated in the course of a formal dispute resolution process.

10. PROVIDE RECOURSE

Responsibilities

Minor Bay is responsible for:

- developing easily accessible and simple complaint procedures and available avenues for recourse;
- informing individuals of avenues of recourse;
- investigating all complaints that are received by the organization;
- correcting personal information practices and policies as is appropriate.

Development of complaint procedures

Developing easily accessible and simple complaint procedures and available avenues for recourse.

Darlene Blue is responsible for developing complaint procedures and will ensure that they are simple and easily accessible.

Avenues for recourse

The avenues for recourse that will be explained in the complaint procedures include:

- complaint procedures within the organization;
- complaint procedures with industry associations;
- complaint procedures with regulatory bodies;
- complaint procedures with the Privacy Commissioner of Canada.

Correcting personal information practices and procedures

The measures that should be followed to correct information handling practices and policies will be set out by ***Darlene Blue***.

Investigation of all complaints received

All complaints must be investigated.

A log book to record complaints must be kept current and include the following categories:

- Date complaint received.
- Nature of complaint (for example, delays in responding to a request, response is inaccurate or incomplete, collection, use or disclosure was improper).
- Receipt of complaint acknowledged (record date).
- Individual asked to clarify complaint (if necessary).
- Name of person assigned to investigate complaint.
- Investigator has access to all relevant records, employees or others who handled the information.
- Individuals notified of results of investigations and any measures that are being taken in light of the outcome.
- Date of outcome.
- Record of all decisions.
- Personal information corrected or modified where inaccuracies or inefficiencies were found and any policies and procedures modified (if necessary).

The person assigned to investigate the complaint must have the skills to conduct a fair and impartial investigation. The investigator must have access to all relevant records, employees and any other person who either handled the personal information or the request for access. Once the investigation is completed, the investigator must clearly and promptly notify the individual of the outcome of the investigation and inform them of any relevant steps that have been taken. Any inaccurate personal information must be corrected. Policies and procedures should be reviewed and modified in response to the outcome of complaints.

Comments and questions welcome

Any comments or questions about this policy should be directed to

Randolph Duvell

1-204-982-9680