



VALLEY HEARTLAND COMMUNITY
FUTURES DEVELOPMENT CORPORATION

PRIVACY POLICY

VALLEY HEARTLAND COMMUNITY FUTURES DEVELOPMENT CORPORATION

TABLE OF CONTENTS

	Page
1.0 PURPOSE OF PRIVACY POLICY	3
1.1 The Ten Principles of <i>PIPEDA</i> Summarized	2
1.2 Personal Information Defined	4
2.0 PURPOSES OF COLLECTING PERSONAL INFORMATION	5
3.0 CONSENT	5
4.0 LIMITING COLLECTION	6
5.0 LIMITING USE, DISCLOSURE AND RETENTION	6
5.1 Use of Personal Information	6
5.2 Disclosure of Personal Information	6
5.3 Retention of Personal Information	7
6.0 ACCURACY	8
7.0 SAFEGUARDS	8
8.0 OPENNESS	9
9.0 INDIVIDUAL ACCESS	9
10.0 COMPLAINTS / RECOURSE	9

Valley Heartland Community Futures Development Corporation

PRIVACY POLICY

1.0 PURPOSE OF VALLEY HEARTLAND COMMUNITY FUTURES DEVELOPMENT CORPORATION PRIVACY POLICY

Valley Heartland Community Futures Development Corporation is a federally supported not-for-profit community organization with a volunteer board of directors and professional staff whose purpose is to develop and diversify local economies. Valley Heartland Community Futures Development Corporation supports community economic development and small business growth by developing and implementing strategic community plans, delivering a range of counselling and information services to small business and operating locally controlled investment funds to provide repayable financing to new and existing businesses.

This privacy policy has been developed to comply with Canada's *Personal Information Protection and Electronic Documents Act* ("PIPEDA"). PIPEDA sets out rules for the collection, use and disclosure of personal information in the course of commercial activity as defined in the Act.

1.1 The Ten Principles of PIPEDA Summarized

The ten Principles of PIPEDA that form the basis of this Privacy Policy are as follows:

1. **Accountability:** organizations are accountable for the personal information they collect, use, retain and disclose in the course of their commercial activities, including, but not limited to, the appointment of a Chief Privacy Officer;
2. **Identifying Purposes:** organizations are to explain the purposes for which the information is being used at the time of collection and can only be used for those purposes;
3. **Consent:** organizations must obtain an Individual's express or implied consent when they collect, use, or disclose the individual's personal information;
4. **Limiting Collection:** the collection of personal information must be limited to only the amount and type that is reasonably necessary for the identified purposes;
5. **Limiting Use, Disclosure and Retention:** personal information must be used for only the identified purposes, and must not be disclosed to third parties unless the Individual consents to the alternative use or disclosure;
6. **Accuracy:** organizations are required to keep personal information in active files accurate and up-to-date;
7. **Safeguards:** organizations are to use physical, organizational, and technological safeguards to protect personal information from unauthorized access or disclosure.

8. Openness: organizations must inform their clients and train their employees about their privacy policies and procedures;
9. Individual Access: an individual has a right to access personal information held by an organization and to challenge its accuracy if need be; and
10. Provide Recourse: organizations are to inform clients and employees of how to bring a request for access, or complaint, to the Chief Privacy Officer, and respond promptly to a request or complaint by the individual.

This Privacy Policy applies to Valley Heartland Community Futures Development Corporation's Board of Directors, members, employees and contracted employees. As well, Valley Heartland Community Futures Development Corporation ensures that all third party service providers sign confidentiality agreements prior to any transfer of an individuals personal information in the course of providing the business loans, business development advice, and other related information and/or services.

1.2 Definitions

"Personal information" means any information about an identifiable individual. It includes, without limitation, information relating to identity, nationality, age, gender, address, telephone number, e-mail address, Social Insurance Number, date of birth, marital status, education, employment health history, assets, liabilities, payment records, credit records, loan records, income and information relating to financial transactions as well as certain personal opinions or views of an Individual.

"Business information" means business name, business address, business telephone number, name(s) of owner(s), officer(s) and director(s), job titles, business registration numbers (GST, RST, source deductions), financial status. Although business information is not subject to *PIPEDA*, confidentiality of business information will be treated with the same security measures by Valley Heartland Community Futures Development Corporation staff, members and Board members, as is required for individual personal information under *PIPEDA*.

"Client" means the business that is applying for or has been approved for a loan, (including sole proprietorships and individuals carrying on business in a partnership);

"Individual" means the client's owner(s) or shareholders, co-signors, and/or any guarantor associated with a client.

"Member" means a person who volunteers on a Valley Heartland Community Futures Development Corporation committee, but who is not a current or active board member, or chair of the committee.

"Application" means the application form or related forms completed by the individual(s) to request financing for the client through the Investment Fund of Valley Heartland Community Futures Development Corporation.

"Data base" means the list of names, addresses and telephone numbers of clients and individuals held by Valley Heartland Community Futures Development Corporation in the forms of, but not limited to, computer files, paper files, and files on computer hard-drives.

"File" means the information collected in the course of processing an application, as well as information collected/updated to maintain /service the account.

"Express consent" means the individual signs the application, or other forms containing personal information, authorizing Valley Heartland Community Futures Development Corporation to collect, use, and disclose the individual's personal information for the purposes set out in the application and/or forms.

"Implied Consent" means the organization may assume that the individual consents to the information being used, retained and disclosed for the original purposes, unless notified by the individual.

"Third Party" means a person or company that provides services to Valley Heartland Community Futures Development Corporation in support of the programs, benefits, and other services offered by Valley Heartland Community Futures Development Corporation, such as other lenders, credit bureaus, persons with whom the individual or client does business, but does *not* include any Government office or department to whom Valley Heartland Community Futures Development Corporation reports in the delivery of such programs, benefits or services.

2.0 PURPOSES OF COLLECTING PERSONAL INFORMATION

Personal information is collected in order to assess the eligibility of the individual completing an application for financial assistance, as well as to report to Industry Canada. The individual is the main source of information but Valley Heartland Community Futures Development Corporation will also ask to obtain information directly from a third source where the individual does not have the required information.

Only that information which is required to make a determination of an individual's eligibility will be collected. Although the individual's Social Insurance Number may be requested in the application for confirming identification of the individual to the credit reporting agency, provision of this personal information is *optional*. The individual may provide alternative forms of identification, such as date of birth and driver's license number.

3.0 CONSENT

An individual's express, written consent will be obtained before or at the time of collecting personal information. The purposes for the collection, use or disclosure of the personal information will be provided to the individual at the time of seeking his or her consent. Once consent is obtained from the individual to use his or her information for those purposes, Valley Heartland Community Futures Development Corporation has the individual's implied consent to collect or receive any supplementary information that is necessary to fulfil the same purposes. Express consent will also be obtained if, or when, a new use is identified.

By signing the application and/or other forms, implied consent is granted by the individual to obtain and/or to verify information from third parties such as banks, credit bureaus, other lenders, and insurance companies in the process of assessing the eligibility of an individual or

client. Implied consent is also granted by the individual to permit Valley Heartland Community Futures Development Corporation to report or otherwise disclose information to Industry Canada, the federal department that administers the Ontario Community Futures Program.

An individual can choose not to provide some or all of the personal information at any time, but if Valley Heartland Community Futures Development Corporation is unable to collect sufficient information to validate the request for financing, the individual's application for such financing may be turned down.

A client or an individual can withdraw consent to Valley Heartland Community Futures Development Corporation's use of personal information at any time prior to the application being approved, by making such request in writing. Once a loan has been approved, an individual cannot withdraw consent authorizing Valley Heartland Community Futures Development Corporation to use and disclose the personal information for the purposes set out in this Privacy Policy. Express consent will be obtained from the individual prior to disclosing the individual's personal information to other lenders, credit insurers and credit bureaus.

This Privacy Policy does not cover statistical data from which the identity of individuals cannot be determined. Valley Heartland Community Futures Development Corporation retains the right to use and disclose statistical data as it determines appropriate.

4.0 LIMITING COLLECTION

Personal information collected will be limited to the purposes set out in this Privacy Policy, Valley Heartland Community Futures Development Corporation applications, and/or other forms.

5.0 LIMITING USE, DISCLOSURE AND RETENTION

5.1 Use of Personal Information

Personal information will be used for only those purposes to which the individual has consented with the following exceptions, as permitted under *PIPEDA*:

Valley Heartland Community Futures Development Corporation will use personal information *without* the individual's consent, where:

- the organization 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;
- an emergency exists that threatens an individual's life, health or security;
- the information is for statistical study or research;
- the information is publicly available;
- the use is clearly in the individual's interest, and consent is not available in a timely way;

- knowledge and consent would compromise the availability or accuracy of the information, and
- collection is required to investigate a breach of an agreement.

5.2 Disclosure and Transfer of Personal Information

Personal information will be disclosed to only those Valley Heartland Community Futures Development Corporation employees, members of Valley Heartland Community Futures Development Corporation committees, and the Board of Directors that need to know the information for the purposes of their work or making an assessment as to the individual's eligibility to the loan program.

Personal information will be disclosed to third parties *with* the individual's knowledge and consent.

PIPEDA permits Valley Heartland Community Futures Development Corporation to *disclose* personal information to third parties, *without* an individual's knowledge and consent, to:

- a lawyer representing Valley Heartland Community Futures Development Corporation;
- collect a debt owed to Valley Heartland Community Futures Development Corporation by the individual or client;
- comply with a subpoena, a warrant or an order made by a court or other body with appropriate jurisdiction;
- a law enforcement agency in the process of a civil or criminal investigation;
- a government agency or department requesting the information; or,
- as required by law.

PIPEDA permits Valley Heartland Community Futures Development Corporation to *transfer* personal information to a third party, *without* the individual's knowledge or consent, if the transfer is simply for processing purposes and the third party only uses the information for the purposes for which it was transferred. Valley Heartland Community Futures Development Corporation will ensure, by contractual or other means, that the third party protects the information and uses it only for the purposes for which it was transferred.

5.3 Retention of Personal Information

Personal information will be retained in client files as long as the file is active and for such periods of time as may be prescribed by applicable laws and regulations.

A file will be deemed inactive if the Investment Committee rejects an application, when a loan is repaid in full and securities are discharged, or when a guarantee is terminated. Information contained in an inactive file will be retained for a period of seven (7) years, except in the case

where an application is rejected. Where an application has been rejected, the file and all personal information contained in the file will be retained for a period of two (2) years.

6.0 ACCURACY

Valley Heartland Community Futures Development Corporation endeavours to ensure that any personal information provided by the individual in his or her active file(s) is accurate, current and complete as is necessary to fulfill the purposes for which the information has been collected, used, retained and disclosed. Individuals are requested to notify Valley Heartland Community Futures Development Corporation of any change in personal or business information.

Information contained in inactive files is not updated.

7.0 SAFEGUARDS

Valley Heartland Community Futures Development Corporation will use physical, organizational, and technological measures to safeguard personal information to only those Valley Heartland Community Futures Development Corporation employees, volunteers, or third parties who need to know this information for the purposes set out in this Privacy Policy.

Organizational Safeguards: Access to personal information will be limited to the Loans Officer, the Administration Officer, and/or the Executive Director who have to make a determination as to the individual's eligibility for a business loan. Personal information provided to members of Valley Heartland Community Futures Development Corporation committee(s) will be limited to only that information required to carry out the mandate of that committee. Members of the Valley Heartland Community Futures Development Corporation committee(s) and/or Board of Directors are not permitted to copy or retain any personal information on individuals or clients and must return for destruction all such information given to them to review once the purpose for being provided with this information has been fulfilled.

Employees and members of Valley Heartland Community Futures Development Corporation committee(s) and/or Board of Directors are required to sign a confidentiality agreement binding them to maintaining the confidentiality of all personal information to which they have access.

Physical Safeguards: Active files are stored in locked filing cabinets when not in use. Access to work areas where active files may be in use is restricted to Valley Heartland Community Futures Development Corporation employees only and authorized third parties.

All inactive files or personal information no longer required are shredded prior to disposal to prevent inadvertent disclosure to unauthorized persons.

Technological Safeguards: Personal information contained in Valley Heartland Community Futures Development Corporation computers and electronic data bases are password protected in accordance with Valley Heartland Community Futures Development Corporation's *Information Security Policy*. Access to any of the Valley Heartland Community Futures Development Corporation's computers also is password protected. Valley Heartland Community Futures Development Corporation's Internet router or server has firewall protection sufficient to protect personal and confidential business information against virus attacks and "sniffer" software arising from Internet activity. Personal information is not transferred to volunteer committee members, the Board of Directors, or third parties by e-mail or other electronic form.

8.0 OPENNESS

Valley Heartland Community Futures Development Corporation will endeavour to make its privacy policies and procedures known to the individual via this Privacy Policy as well as the Valley Heartland Community Futures Development Corporation *Privacy Statement*. This document will also be available on Valley Heartland Community Futures Development Corporation's website: www.valleycfdc.com.

9.0 INDIVIDUAL ACCESS

An Individual who wishes to review or verify what personal information is held by Valley Heartland Community Futures Development Corporation, or to whom the information has been disclosed (as permitted by the *Act*), may make the request for access, in writing, to the Valley Heartland Community Futures Development Corporation's Chief Privacy Officer. Upon verification of the individual's identity, the Chief Privacy Officer will respond within 60 days.

If the individual finds that the information held by Valley Heartland Community Futures Development Corporation is inaccurate or incomplete, upon the individual providing documentary evidence to verify the correct information, Valley Heartland Community Futures Development Corporation will make the required changes to the individual's active file(s) promptly.

10.0 COMPLAINTS/RECOURSE

If an individual has a concern about Valley Heartland Community Futures Development Corporation's personal information handling practises, a complaint, in writing, may be directed to the Valley Heartland Community Futures Development Corporation's Chief Privacy Officer.

Upon verification of the individual's identity, Valley Heartland Community Futures Development Corporation's Chief Privacy Officer will act promptly to investigate the complaint and provide a written report of the investigation's findings to the individual.

Where Valley Heartland Community Futures Development Corporation's Chief Privacy Officer makes a determination that the individual's complaint is well founded, the Chief Privacy Officer will take the necessary steps to correct the offending information handling practise and/or revise Valley Heartland Community Futures Development Corporation's privacy policies and procedures.

Where Valley Heartland Community Futures Development Corporation's Chief Privacy Officer determines that the individual's complaint is *not* well founded, the individual will be notified in writing.

If the individual is dissatisfied with the finding and corresponding action taken by Valley Heartland Community Futures Development Corporation's Chief Privacy Officer, the individual may bring a complaint to the Federal Privacy Commissioner at the address below:

The Privacy Commissioner of Canada
112 Kent Street, Ottawa
Ontario K1A 1H3
Tel 1-800-282-1376

Email address: www.privcom.gc.ca.

Questions/Access Request/Complaint

Any questions regarding this or any other privacy policy of Valley Heartland Community Futures Development Corporation may be directed to the Chief Privacy Officer. Requests for access to information, or to make a complaint, are to be made in writing and sent to the Chief Privacy Officer at the address below:

Chief Privacy Officer
Valley Heartland Community Futures Development Corporation
91 Cornelia Street West
Smiths Falls, ON K7A 5L3

Email address: valley@valley.on.ca

Amendment to Valley Heartland Community Futures Development Corporation's Privacy Policies

This Valley Heartland Community Futures Development Corporation's Privacy Policy is in effect April 20, 2004 and is retroactive to January 1, 2004. This policy is subject to amendment in response to developments in the privacy legislation. The Chief Privacy Officer will review and revise the Privacy Policy from time to time as required by changes in privacy law. Notification of any changes in the Privacy Policy will be posted on Valley Heartland Community Futures Development Corporation's website, as well as in Valley Heartland Community Futures Development Corporation's Privacy Statement. Any changes in the Privacy Policy will apply to Personal information collected from the date of the posting of the revised Privacy Policy on Valley Heartland Community Futures Development Corporation's website: www.valleycfdc.on.ca.

VALLEY HEARTLAND COMMUNITY FUTURES DEVELOPMENT CORPORATION

PRIVACY STATEMENT

INTRODUCTION

Valley Heartland Community Futures Development Corporation (VHCFC) is a federally supported not-for-profit community organization with a volunteer Board of Directors and professional staff whose purpose is to support community economic development and small business growth through business loans or loan guarantees.

This brochure summarizes VHCFC's privacy policies and procedures that have been developed to comply with Canada's *Personal Information Protection and Electronic Documents Act* ("PIPEDA"). PIPEDA sets out rules for the collection, use and disclosure of a client's or customer's personal information, as well as safeguarding that information in the course of commercial activity as defined in the legislation.

WHAT IS "PERSONAL INFORMATION"

Under PIPEDA, "Personal Information" means any information that is identifiable to an individual, including name, address, telephone number, Social Insurance Number, and date of birth. It also includes, but is not limited to, other information relating to identity, such as, nationality, gender, marital status, financial information and credit history.

PURPOSES FOR PERSONAL INFORMATION

VHCFC collects only that personal information required to assess a prospective applicant's eligibility for financial assistance, as well as to report to Industry Canada, the federal department

that administers the Ontario Community Futures Program.

CONSENT

At the time of completing a loan application, the express, written consent of the individual applicant will be sought for the collection, use, retention and disclosure of their personal information for the purposes set out in VHCFC's privacy policy.

An applicant may choose not to provide some or all of the personal information requested, but if VHCFC is unable to collect sufficient information to validate a financing request, the application for financing may be turned down.

ACCURACY

VHCFC endeavours to ensure that all personal information in active files are accurate, current and complete. When a client notifies VHCFC that his or her personal information requires correction or updating, the necessary changes will be made. Information contained in closed files is not updated.

LIMITING USE, RETENTION & DISCLOSURE

VHCFC uses and retains personal information for only those purposes to which the individual has consented.

Personal information will be disclosed to only those VHCFC employees, volunteer members of committees and/or Board of Directors that need to know the information for the purposes set out in the VHCFC Privacy Policy.

SAFEGUARDS

VHCFC utilizes a number of physical, organizational and technological measures to

safeguard personal information from unauthorized access or inadvertent disclosure in accordance with its *Information Security, Retention and Destruction Policy*, including but not limited to:

Physical

Active files are stored in locked filing cabinets located in work areas restricted to VHCFC employees and authorized volunteers. Closed files are stored in locked cabinets for a period of seven years, after which, the information is shredded prior to disposal.

Organizational

VHCFC employees, volunteers, and third party service providers sign confidentiality agreements binding them to safeguarding the confidentiality of personal information to which they have access.

Technological

Personal information contained on VHCFC computers and the electronic database are password protected. As well, the Internet server or router has firewall protection to protect against virus attacks and hacking into the database.

Electronic Transmission of Information

Notwithstanding the technological safeguards implemented by VHCFC, all Internet transmissions are susceptible to possible loss, misrouting, interception and misuse. For this reason, as part of the application that individual's sign consenting to their personal information being collected, used, retained, and disclosed, VHCFC will assume that it has the individual's consent to communicate via the Internet unless notified to the contrary.

INDIVIDUAL ACCESS

An individual who wishes to review or verify what personal information is held by VHCFCDC, may do so by making a request, in writing to the VHCFCDC's Chief Privacy Officer. Upon verification of the individual's identity, the Chief Privacy Officer will provide a written report within 60 days.

INVESTIGATING COMPLAINTS

Any concern or issue about VHCFCDC's personal information handling practises may be made, in writing, to the Chief Privacy Officer. Upon verification of the individual's identity, the Chief Privacy Officer will act promptly to investigate the complaint and provide a written report to the individual.

If the individual is dissatisfied with the report provided by the Chief Privacy Officer, or feels that the corrective action taken by VHCFCDC is insufficient, the individual may direct a complaint to the Federal Privacy Commissioner in writing. The address of the Federal Privacy Commissioner is provided in this Privacy Statement for your convenience.

AMENDMENTS TO OUR PRIVACY POLICY

This Privacy Statement is a summary of VHCFCDC's Privacy Policy. For full particulars of VHCFCDC's privacy policies and procedures, please request a copy of the Privacy Policy from VHCFCDC or a copy may be obtained from the Internet website at: www.valleycfdc.com.

The VHCFCDC Privacy Policy and this Privacy Statement are in effect April 20, 2004 and is retroactive to January 1, 2004. VHCFCDC's Privacy Policy and this Privacy Statement may be updated from time to time to reflect amendments in applicable Federal and Provincial laws. Any

changes to this Privacy Policy will be posted on VHCFCDC's website and will apply to personal information collected from the date of the posting of the revised Privacy Policy.

CONTACT INFORMATION

If you have any questions regarding VHCFCDC's Privacy Policy, Information Security, Retention and Destruction Policy, and/or this Privacy Statement, or you wish to make an access to personal information request, please contact:

Chief Privacy Officer valley@valley.on.ca
Valley Heartland CFDC
91 Cornelia St. W.
Smiths Falls, Ontario K7A 5L3
Phone: 613-283-7002 Facsimile: 613-283-7005

OTHER HELPFUL PRIVACY LINKS

For a copy of *PIPEDA*, or for answers to other questions regarding privacy legislation, below are some helpful privacy links.

Federal Privacy Commissioner
www.privcom.gc.ca
112 Kent Street
Ottawa, ON K1A 1H3

Provincial Privacy Commissioner
www.privcom.on.ca

VHCFCDC Privacy Policy Web Site:
www.valleycfdc.com

Siskind, Cromarty, Ivey & Dowler LLP
Privacy Law Group:
www.siskindsprivacylaw.com



**VALLEY HEARTLAND
COMMUNITY FUTURES
DEVELOPMENT
CORPORATION**

PRIVACY STATEMENT

VALLEY HEARTLAND COMMUNITY FUTURES DEVELOPMENT
CORPORATION
Information Security Policy

1.0 General	1
2.0 Definitions.....	1
3.0 Information Security Requirements.....	2
3.1. Privacy & Confidentiality	2
3.2. Valley Heartland CFDC Property	3
3.3. Identification & Authentication	3
3.4. Use of Valley Heartland CFDC Computers	4
3.5. Access to Valley Heartland CFDC Information or Computers	5
3.6. Software	5
3.7. Internet Communications.....	5
3.8. Physical Security	7
3.9. System Risk Management	7
3.10. Monitoring	7
4.0 Exceptions to Policy.....	8
5.0 Non-compliance With Policy	9
Annex A - Password Standards.....	10

1.0 General

The Valley Heartland Community Futures Development Corporation (“Valley Heartland CFDC”) has adopted this Information Security Policy to ensure that adequate protection measures are taken to assure the confidentiality and integrity of the information held by Valley Heartland CFDC and the security of the computer system to include hardware, software, and storage devices such as disks, CDs and backup systems.

This Policy applies to Users with respect to their access to, and use of, Valley Heartland CFDC- held information as well as access to hardware, software or network facilities owned or controlled by Valley Heartland CFDC. With respect to employees, this Policy is also to be read in conjunction with and form a part of Valley Heartland CFDC’s *Employee Handbook*. All new employees and contractors shall receive a copy of this Policy upon employment or engagement.

In the event of questions about this Policy, please contact:

Chief Privacy Officer
Valley Heartland CFDC
91 Cornelia Street W.
Smiths Falls, Ontario
K7A 5L3

E-mail: info@valley.on.ca
Telephone number: 613-283-7002
Fax: 613-283-7005

2.0 Definitions

“Availability” means information being accessible as required.

"Confidential Information" means Personal Information; Valley Heartland CFDC business, tax or accounting information; employee information and disciplinary files, and archived information pertaining to former members or employees.

"Confidentiality" means the restriction of access to information only to those having a business reason to have such access as authorized by the appropriate manager within Valley Heartland CFDC or the client concerned. Exceptions should be forwarded to the Chief Privacy Officer.

"Disruption of network communication" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

"Integrity" means the information in question has not been modified in an unauthorized manner.

"Internet communications" means existing and future communication protocols and services including but not limited to the World Wide Web; electronic mail ("e-mail"); Instant Messaging; Internet Relay Chat; any intranet that Valley Heartland CFDC establishes or participates in; any proprietary data transfer protocols utilized by Valley Heartland CFDC in communications with others; File Transfer Protocol, TELNET and Usenet news groups.

"Members" mean an employee, officer, director or other type of member of Valley Heartland CFDC.

"Personal Information" means any information, recorded in any form, about an identified individual, or an individual whose identity may be inferred or determined from the information.

"Security breaches" means accessing data of which the User is not an intended recipient or logging into a server or account that the User is not expressly authorized to access, unless these activities are within the scope of regular duties.

"User" means an individual, whether an employee, officer, director or other type of member of Valley Heartland CFDC who creates or accesses information on Valley Heartland CFDC-owned or controlled Computer System; or a computer program or application operating pursuant to an individual or organization (e.g. electronic agent).

3.0 Information Security Requirements

3.1. Privacy & Confidentiality

Users with access to Personal Information shall respect the confidentiality of that information and adhere to the requirements of Valley Heartland CFDC's *Privacy Policy* and Valley Heartland CFDC's *Employee Information Privacy Policy*.

Users with access to other types of Confidential Information shall respect the confidentiality of that information and not disclose such information unless specifically authorized to do so.

Each User that accesses information held by Valley Heartland CFDC, whether owned by Valley Heartland CFDC or not, regardless of form (e.g. paper or electronic) or format, shall protect that information against accidental or deliberate disclosure or destruction. Modification to the information shall be completed as per established and accepted Valley Heartland CFDC policies and procedures.

Confidential Information shall be:

- Physically protected through the use of locked cabinets or offices and/or technologically protected using Computer System access controls;
- Accessible for review by employees as authorized by Valley Heartland CFDC management;
- Corrected or marked with appropriate notation in the event inaccuracies in the information are identified; and
- Retained for such retention periods as required by law or as identified by Valley Heartland CFDC management.

3.2. Valley Heartland CFDC Property

All information and/or messages composed, sent or received using Valley Heartland CFDC's computers are the property of Valley Heartland CFDC and may be reviewed, audited, accessed and disclosed for any purpose considered appropriate by Valley Heartland CFDC management. **USERS SHOULD NOT HAVE ANY EXPECTATION OF PRIVACY WITH RESPECT TO SUCH MESSAGES.** See also Section 3.10 Monitoring.

Unless contractual or licensing arrangements govern, any data or software downloaded using Internet communications into Valley Heartland CFDC computers becomes the property of Valley Heartland CFDC and may be retained, removed or destroyed at the sole discretion of Valley Heartland CFDC management.

3.3. Identification & Authentication

Each User shall be assigned a unique identifier ("User ID") and will be required to authenticate themselves prior to gaining access to Valley Heartland CFDC computers or networks. Users shall not log on to Valley Heartland CFDC computers using another User's User ID. **EACH USER SHALL BE RESPONSIBLE FOR ALL ACTIVITY CONDUCTED UNDER THEIR ASSIGNED USER ID.**

Associated with each User ID will be a password generated to authenticate a User prior to accessing any application, system, network or remote connection. A User shall adhere to the requirements of Annex A Password Standard. All default passwords and access codes on vendor-supplied hardware and software shall be changed prior to use by Users.

The System Administrator shall have a separate Administrator User ID and password. Administrator User IDs shall only be used for system administration purposes.

The Administrator's User ID and password shall be changed immediately upon (a) the installation of any system; and (b) immediately after use by service personnel. The administrator's password shall be documented and stored in a secure location.

Where non-specific User accounts are required, they shall be assigned to a specific User for accountability purposes. The purpose of the account shall be documented and the password associated with the account changed when a User who knows the password is no longer an employee or a contractor of Valley Heartland CFDC.

User IDs shall be deleted from a Valley Heartland CFDC computer upon the termination of a User's employment or, in the case of contractors, contract. User IDs that are inactive for thirty days shall be disabled and removed.

3.4. Use of Valley Heartland CFDC Computers

The Valley Heartland CFDC shall provide employees and managers, and may (but is not required to) provide other Users, with workstations for the purposes of their activities with the Valley Heartland CFDC. **USERS SHALL BE RESPONSIBLE AND ACCOUNTABLE FOR THEIR ACTIONS while using Valley Heartland CFDC hardware, software or networks, or components thereof, including desktop or laptop computers or personal digital assistants (PDAs) owned, leased or controlled by Valley Heartland CFDC.**

Users shall use Valley Heartland CFDC computers primarily for business purposes. Limited and reasonable personal use of the Valley Heartland CFDC computers is permitted provided such use:

- a. Is not for non-Valley Heartland CFDC commercial purposes or personal gain;
- b. Does not:
 - i) Adversely affect the primary business use of the computer or Valley Heartland CFDC network;
 - ii) Conflict with a Valley Heartland CFDC business objective or policy;
 - iii) Consume a large amount of Valley Heartland CFDC computer resources;
- c. Complies with applicable law.

Valley Heartland CFDC management shall be solely responsible for any determination as to what constitutes limited and reasonable personal use.

Under no circumstances is a User authorized to engage in any activity that is illegal under the laws of Ontario and Canada while utilizing the Valley Heartland CFDC computers.

Users shall not harm or destroy, or attempt to harm or destroy, hardware, software or data on any Valley Heartland CFDC computer, other than their own data in the course of editing such material.

Users shall not load, install or activate, or attempt to load, install or activate onto Valley Heartland CFDC computers any unauthorized hardware, including, but not limited to, modems, data scopes, line monitors, nodes, gateways or bridges of any kind.

Users of Valley Heartland CFDC-owned or controlled portable devices (e.g laptops, PDAs), if supplied with such equipment, shall not leave such equipment unattended when outside Valley Heartland CFDC offices. Information contained on such devices must be protected from unauthorized access using power-on passwords or passphrases and password or passphrase-enabled time-out or lock-out features.

3.5. Access to Valley Heartland CFDC Information or Computers

User access to Valley Heartland CFDC information or to Valley Heartland CFDC computers shall be on an "as authorized" basis in order to accomplish Valley Heartland CFDC business objectives. Networks shall have routing controls to ensure connections and information flows do not have unauthorized access to Valley Heartland CFDC information.

Any computer or portable device with a modem operating in "inbound mode active" (permitting external callers to connect to the device using that modem) shall not be simultaneously connected to both a Valley Heartland CFDC network and any external network.

3.6. Software

Only software approved for deployment by Valley Heartland CFDC management is permitted on any Valley Heartland CFDC computer or network. Downloading software programs (e.g. screen savers, audio software and messaging software) from the Internet is not permitted. All other file types downloaded from the Internet must be scanned with anti-virus software before being stored on Valley Heartland CFDC computers. If a User has a business requirement to download software from the Internet or to otherwise load non-Valley Heartland CFDC standard software, Section 4.0 Exceptions to Policy will govern.

Virus detection software shall be installed and regularly updated on Valley Heartland CFDC computers and networks. Users are required to report any known or suspected virus incidents to the System Administrator.

Opening e-mail attachments with ".exe" or ".com" extensions (including trial versions of software) is not permitted.

Any application to be purchased, whether custom-developed or commercially available, shall have authentication and access controls. The application should ensure that, with respect to the information it stores, the application shall maintain the integrity of the data.

Users shall report any observed or suspected software malfunctions but shall not attempt to remove the software in question unless authorized to do so.

3.7 Internet Communications

Valley Heartland CFDC may provide all Users with Internet access for business and limited personal purposes. Valley Heartland CFDC may also provide e-mail addresses

with "@valleycfdc.com" to employees. Accordingly, the use of Valley Heartland CFDC resources that identify a user with Valley Heartland CFDC must be done in a manner that reflects well on the organization. All access to the Internet shall be done via approved Valley Heartland CFDC gateways and in a manner consistent with this Policy. Managers and employees must understand that Internet access is to be treated as a privilege that may be revoked at any time in the event of a failure to comply with this Policy. Withdrawal of access to the Valley Heartland CFDC network or the Internet may occur whether or not disciplinary action is taken.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use of Valley Heartland CFDC's computers. In the absence of applicable Valley Heartland CFDC policies or if there is any uncertainty, users should consult their General Manager or the Chief Privacy Officer.

The following system and network activities are expressly prohibited:

1. Installing or distributing "pirated" or other software products that are not appropriately licensed for use by Valley Heartland CFDC;
2. Copying and/or distributing material not authorized by Valley Heartland CFDC management including, but not limited to, music, text or photographs from magazines, books or other copyrighted sources;
3. Providing information about, or lists of, Valley Heartland CFDC employees to parties outside Valley Heartland CFDC;
4. Introducing malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.);
5. Using an Valley Heartland CFDC computer to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws under the laws of Ontario and Canada;
6. Making fraudulent offers of products, items, or services;
7. Making statements about warranty, expressly or implied, unless it is a part of normal job duties;
8. Causing security breaches or disruptions of network communication;
9. Intercepting data not intended for the User's host computer, unless this activity is a part of the employee's normal job/duty;
10. Circumventing user authentication or security of any computer or network account;
11. Interfering with or denying service to any user other than the user's host (for example, denial of service attack);
12. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's use of a computer;
13. Exporting or importing software, technical information, encryption software or technology, in violation of applicable Canadian import and export control laws; and
14. Using an unassigned "User ID" and/or password.

The following communication activities are strictly prohibited:

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material;

2. Harassing Valley Heartland CFDC employees or employees of members or third parties via email, telephone or paging, whether through language, frequency, or size of messages;
3. Forging email header information;
4. Soliciting email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies;
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type; and
6. Posting the same or similar non-business-related messages to large numbers of newsgroups or web sites.

Users may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

3.8 Physical Security

Computers located within Valley Heartland CFDC are to be located in areas that have appropriate physical security controls, including but not limited to, keys or combination locks, access logs and alarms. Users whose employment or contract is terminated shall return all keys assigned to them. A log of office keys shall be maintained by the Chief Privacy Officer who shall also have responsibility for the issuance and retrieval of keys.

Storage media shall be protected from environmental threats such as temperature, humidity and magnetism. All media containing Confidential Information shall be sanitized or destroyed before release for disposal to ensure that data recovery from such media is not possible.

Equipment shall not be removed from the Valley Heartland CFDC offices or facilities without permission.

3.9 System Risk Management

Any new computer system or modification to existing Valley Heartland CFDC computers or network shall be assessed for risk prior to deployment. Such a risk assessment shall examine any potential consequences of a loss of confidentiality, integrity or availability of Valley Heartland CFDC information or other assets, and the realistic likelihood of a loss occurring in the light of prevailing threats and vulnerabilities, and the controls currently implemented. This risk assessment may be completed by the System Administrator or such person(s) as the General Manager believes is appropriate to conduct such an assessment.

3.10 Monitoring

The Valley Heartland CFDC reserves the right to monitor computers or networks to ensure compliance with this Policy. For security and network maintenance purposes, authorized individuals within Valley Heartland CFDC may monitor and access equipment, systems and network traffic at any time.

Such access may include:

- User level and/or system level access to any computing or communications device;
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on Valley Heartland CFDC computers or property;
- Access to work areas (offices, cubicles, storage areas, etc.).

For Valley Heartland CFDC computers important to the activities of Valley Heartland CFDC, at a minimum, the following information shall be recorded either electronically or manually:

- Login and logout attempts;
- Unauthorized attempts to access system files;
- Attempts to create, remove, set passwords or change the system privileges of system administrators;
- System alerts or failures; and
- System configuration changes and maintenance information.

All logs, whether electronic or manual, must contain the date and time of the event and the User ID which caused the event and are to be reviewed, at a minimum, on a monthly basis.

Where a computer records information that is required to be logged and operates a clock, that computer's clock should be set, as required, to Standard Time or Daylight Savings Time in Ontario. Computer system clocks shall be checked every 60 days as to their accuracy.

Logs are to be protected against unauthorized changes or operational failures (e.g. logging media exhausted; failing to record events or overwriting itself).

Monitoring tools and systems audit processes are to be configured so as to only allow designated personnel to change such tools and processes.

Audit logs shall be archived monthly and retained according to Valley Heartland CFDC's *Records Retention Policy*.

Security processes and controls are to be audited annually.

4.0 Exceptions to Policy

Exceptions to any policy requirement stated in Section 3 may be permitted if:

- An appropriate business reason is provided;
- The request is approved by the General Manager or Chief Privacy Officer; and
- The User making the request accepts all responsibility for any additional risk created by the exception.

5.0 Non-compliance With Policy

While records of communications can be created for monitoring and review purposes, Valley Heartland CFDC will not actively monitor the communications of users. However, the Valley Heartland CFDC may do so upon suspicion or evidence of a breach of any law or the Valley Heartland CFDC policy and any past communication may be examined in the course of an investigation of a security breach or in the course of disciplinary action. See Section 3.2.

Any user who disregards, disobeys, disables or circumvents any element of this Policy or any security mechanism, or who attempts to do so, shall be subject to disciplinary action, up to and including termination of employment or, in the case of contractors, termination of contracts. Users should also note that, if circumstances warrant, an incident may be referred to the appropriate authorities for prosecution.

Valley Heartland CFDC reserves the right to restrict any user's access to Valley Heartland CFDC information or computers.

Agreements with external vendors or suppliers shall require compliance with this Policy in the event of use of Valley Heartland CFDC computers or networks by such vendors or suppliers, or employees or agents, thereof.

Annex A – Password Standards

- 1) Passwords should never be written down or stored on-line. ***
- 2) Do not use the same password for Valley Heartland CFDC accounts as for other non-Valley Heartland CFDC accounts (e.g., personal ISP account).
- 3) Where possible, don't use the same password for different access needs within the Valley Heartland CFDC systems. For example, select a separate password to be used to access the TEA network as is used for access to Windows.
- 4) All passwords are to be treated as sensitive, Board Confidential Information.
- 5) Do not hint at the format of a password in any conversation or communication (e.g., "my family name").
- 6) Do not use the "Remember Password" feature of applications (e.g., Eudora, Outlook, Netscape Messenger).
- 7) Do not reveal a password:
 - a) Over the phone to ANYONE;
 - b) In an email message;
 - c) In front of others;
 - d) To family members or co-workers; or
 - e) On questionnaires or forms.

*** Alternative solution

- 1) Individuals could write down their passwords, place them in a sealed envelope with their name and the date and provide these to the Chief Privacy Officer for storage in a locked fire-proof cabinet. The process is then undertaken each and every time an individual changes any of their passwords.

VALLEY HEARTLAND COMMUNITY FUTURES DEVELOPMENT CORPORATION

Record Retention & Destruction Policy

1.0	Objectives and Scope of Policy	1
2.0	Roles and Responsibilities	2
3.0	Transitory Records	2
4.0	Development of Retention Requirements	3
5.0	Record Retention or Destruction	4
6.0	Electronic Documents	6
	6.1 Electronic Document Types and Guidelines	6
	6.2 Compliance	7
7.0	Suspension of the Destruction or Disposal of Records	7
8.0	Enquiries	7
Annex A		8
Annex B		12
Annex C		13

1.0 Objectives and Scope of Policy

The Valley Heartland Community Futures Development Corporation ("Valley Heartland CFDC") has prepared this Policy Statement to outline Valley Heartland CFDC's policy concerning the retention and destruction of records within the control of the Corporation. The Corporation wishes that decisions as to how long records are kept are made and applied in a systematic fashion. This is done in order to permit Valley Heartland CFDC to:

- Identify, protect, and preserve those records that need to be kept to meet business, legal, or historical requirements;
- Reduce Valley Heartland CFDC costs;
- Better manage Valley Heartland CFDC computer facilities by;
 - Eliminating the storage of unnecessary information on the Valley Heartland CFDC computer network or employee desktops;
 - Encouraging optimal performance of the Valley Heartland CFDC computer network;
 - Eliminating confusion over different iterations of documents;
 - Ensuring that important documents are not made unusable by technological upgrades; and
 - Ensuring, to the degree possible, the authenticity of electronic documents on the network and the employees' desktops;
- Protect Valley Heartland CFDC employees and management from the risks associated with the inadvertent or inappropriate destruction of Valley Heartland CFDC assets; and
- Support the protection of sensitive information by ensuring records are disposed of in an appropriate fashion.

For the purposes of this policy, records are defined as any recorded information that is created or received by any individual, whether employed or contracted by Valley Heartland CFDC, in the course of conducting Valley Heartland CFDC business. It is particularly important to note that such records are the

property of Valley Heartland CFDC and not the employee or contractor who created or received them. It is equally important to note that the definition of records applies regardless of the format or medium of the information. This would include paper, film, and electronic formats, such as text, image, voice, video, graphics, or e-mail messages – whether work-related or personal - created and/or stored on Valley Heartland CFDC desktop/laptop machines, personal digital assistants (should they be provided by Valley Heartland CFDC) or the TEA network. See Section 5.0 concerning electronic documents.

Final disposition of a record typically occurs through physical destruction or transfer to the Valley Heartland CFDC archives. When and how individual documents are disposed of depends on the retention requirements that are established for each set of records. These are defined by a variety of different factors, including both business needs and any statutory record keeping requirements.

2.0 Roles and Responsibilities

The General Manager, in conjunction with the Chief Privacy Officer, is responsible for ensuring that the records produced by Valley Heartland CFDC, in the course of the Corporation conducting its business, are managed according to Valley Heartland CFDC policies and standards. This includes ensuring that appropriate retention requirements are defined and applied in the disposition of records.

The Chief Privacy Officer is also responsible for supporting the managers and employees in Valley Heartland CFDC Departments in the retention and disposition of records by providing guidelines and by facilitating the actual disposition of records. This formal and controlled disposition process provides evidence that Valley Heartland CFDC has exercised due diligence in the destruction of records.

With respect to records, managers are to ensure that they and the employees for which they are directly responsible comply with this policy. Employees have two key responsibilities under this Policy. First, is to treat transitory records in a manner consistent with this policy. Second, is to submit all other records to a reliable record-keeping system so that they can be disposed of in accordance with Valley Heartland CFDC standards.

3.0 Transitory Records

No records should be destroyed by individual employees with the exception of those that are transitory. Transitory records are defined as those that:

- Are not of enduring value;
- Are not needed for statutory, legal, fiscal, administrative, operational or archival purposes;
- Are needed only for a limited period of time (usually a week or less) to complete a routine action or the preparation of a record; and
- Are not regularly filed in a records or information system.

Transitory records may be considered as falling into seven general categories:

- Temporary information;
- Duplicates;
- Draft documents and working materials;
- Publications;
- Direct mail;

- Blank information media; and
- Personal notes.

Temporary information includes telephone messages, routing slips, post-it notes, opened envelopes, memos, notes and messages (either paper, voice or electronic) where the information has only immediate or very short-term value. Once they have been used to perform the required activities, the records have no further value and may be destroyed.

However, it is to be noted that records like this may need to be kept. For example, envelopes might be kept because the time and date of receipt are stamped on them. A telephone message slip may have to be filed as it provides evidence of an individual calling at a certain time and date. If there is any doubt about whether recorded information will have any further reference value, file the record.

Duplicates are exact reproductions of a master document. Examples of such records include photocopies, or extra copies printed from a computer system or by a commercial printer. After the master version of a document has been filed, duplicates that are no longer needed may be discarded. Duplicates that are circulated strictly for reference purposes should be clearly identified so they will not be filed. An important caveat to note is that a duplicate is sometimes altered by someone adding handwritten or electronic notes to it. This action creates a new record. If this added information is substantive and will have future value, file the document as a new record.

Draft documents and working materials includes source materials used in the preparation of documents and earlier versions of final documents. Usually, drafts and working materials, whether paper or electronic, do not have long-term value and can be discarded as transitory records. However, exceptions to this general rule do exist: drafts and working papers related to the preparation of legal documents, budgets, policies, standards, guidelines and procedures may not be transitory. If a manager believes that the information contained in such a record may have some future value to Valley Heartland CFDC then that record should be filed. If any employee is unsure as to the future value of a record, he or she should consult their manager.

Publications include books, magazines, periodicals, pamphlets, brochures, journals, newspapers and software documentation obtained from sources outside Valley Heartland CFDC. If they will have no future value, they can be discarded once a manager or employee is finished with them. The master copy of any publication produced by Valley Heartland CFDC is not transitory and should be filed.

Direct mail includes solicited or unsolicited information received from organizations or individuals advertising their products or services. The vast majority of such mail may be considered junk mail and may be discarded.

Blank information media includes anything that was created or acquired for the purpose of collecting or storing information but which has not been used and has become obsolete. Obsolete blank forms are a good example. This category also includes storage media such as video, audio, or dictation tapes, diskettes, magnetic tapes, disk drives, or optical disks, where sensitive or confidential information was previously stored or where that information was erased; and where it is possible that someone could recover the erased information by technical means. Such "non-paper" items are either to be physically destroyed or erased in a secure manner by "overwriting".

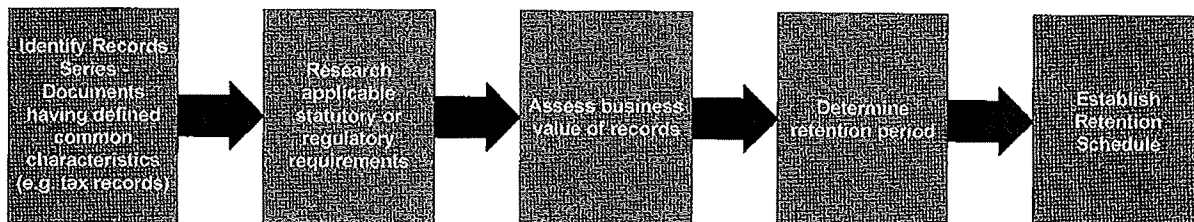
Personal notes include messages which are not directly related to the work of employees but does not include personal information needed for purposes of personnel management.

4.0 Development of Retention Requirements

Because this policy is designed to facilitate the routine, orderly and timely archiving or disposition of records by Valley Heartland CFDC managers and employees, it may become apparent that this policy fails to address certain classes of documents since new types of records or new media to hold records may be created over time. Accordingly, Annex A of this Policy may require amendment over time. This

should be brought to the attention of the Chief Privacy Officer who shall determine (or have determined) the retention period for the record or class of records in accordance with the process described below.

This process of developing retention and disposal requirements is comprised of a small number of steps. As depicted below, the process begins with the identification of a series of records which represent broad categories of information that share common management requirements.



The research element is to identify any statutes or regulations that might apply to each records series. Some statutes outline very clear retention requirements for particular kinds of records, such as the *Income Tax Act*. Others identify more general requirements to create and retain records, but do not identify a specific time frame. One or more statutes may apply to any given set of records – sometimes with conflicting retention requirements which must be reconciled.

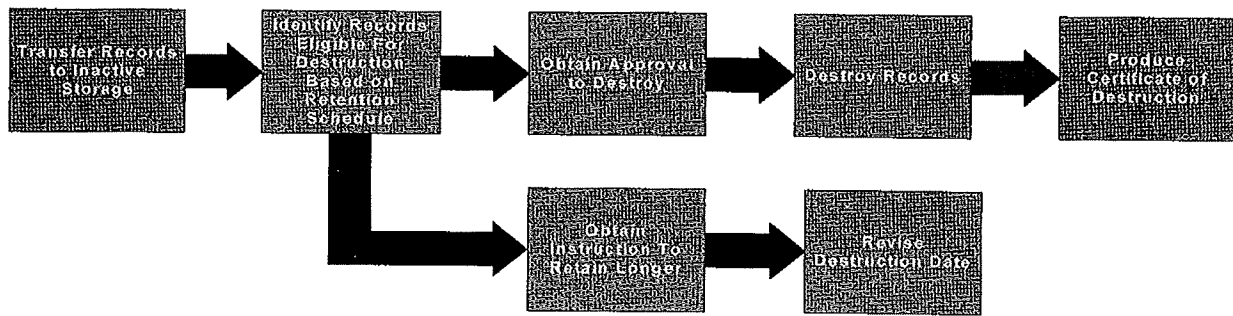
Once the research is completed, and whether or not there is a legal requirement, Valley Heartland CFDC's business needs to retain the record is assessed. This is especially important in the absence of any legal requirement to retain. The specific retention periods, reflecting both business needs and any statutory and regulatory requirements, are then fixed. The retention requirements that result from this process are documented within the "Record Retention Schedule" which becomes the official guideline for how long records are to be kept.

Valley Heartland CFDC's development of a retention/disposition schedule is generally a one-time activity that addresses the broad administrative, financial, legal, audit and historical value of the Corporation's record holdings. If records do not fit within existing categories of documentation then the process outlined above is to be employed. A copy of the current retention schedule for Valley Heartland CFDC documents is attached as Annex A.

5.0 Record Retention or Destruction

The attached Annex A has guidelines for the appropriate retention of numerous types of records. Records will ordinarily be kept in the Department creating a document unless otherwise directed to be stored elsewhere. If, after consulting this policy and the schedule attached, there exists a question regarding the proper disposition or retention of a particular document or class of documents, it shall be the responsibility of the head of the department in possession of the document to determine the proper disposition of the item or items in consultation with the Chief Privacy Officer.

Application of the retention schedule occurs upon the disposition of actual record holdings. Most often this involves reviewing records that have been transferred to "inactive storage" to determine those that are eligible for physical destruction or transfer to the Valley Heartland CFDC's archives. The following diagram illustrates the process that is followed in applying the guidelines found in Annex A to Valley Heartland CFDC record holdings.



At least once a year, using the retention schedule in Annex A as a guideline, all files that are scheduled to be destroyed are to be listed. The list is provided to the General Manager who will either approve final destruction or advise whether they should be retained for an additional period of time. This process serves as a final check on the initial retention decision and also allows for the application of any changes in requirements.

Once approval to destroy is obtained, records are to be physically destroyed and the Certificate of Destruction, in the form contained in Annex B, is completed and filed in the Chief Privacy Officer's Office. This provides a record of what has been destroyed and is used as an audit trail if destruction practices are questioned.

Paper or electronic records, other than sensitive, financial or confidential records, may be disposed of in the following manners:

- Recycling;
- Shredding;
- Placement in garbage for regional landfill;
- Physically destroyed; or
- Erased in a secure manner by overwriting.

Sensitive, financial or confidential records must to be shredded or erased in a secure manner before disposal. What constitutes "sensitive" information is left to be determined at the discretion of the manager concerned or the Chief Privacy Officer who are to err on the side of caution if there is any doubt as to the sensitivity of any information scheduled for disposition.

No employee is to retain any "private" or "secret" files. Retention of such files is grounds for dismissal.

No tape recordings are to be retained. Meetings, other than hearings, may only be taped with the approval of the Chief Privacy Officer and such tapes must be erased immediately after the preparation of the report.

Employees who knowingly destroy, without authorization, any of the Corporation documents will be immediately suspended pending an inquiry by the Chief Privacy Officer, the employee may be subject to disciplinary measures up to and including termination. If it is found that the employee knowingly destroyed documents related to litigation or to complaints, the employee will be subject to disciplinary measures up to and including termination.

6.0 Electronic Documents

With respect to their obligations in retaining electronic documents - including e-mail, Web files, text files, PDF documents, and all other formatted files - managers and employees are to refer to this section of the record retention policy.

6.1 Electronic Document Types and Guidelines

Unless otherwise listed for retention in Annex A and subject to Section 7.0, the following are the types of electronic documents covered under this policy and the corresponding period of time in which each document should be retained. Other formats may be added as necessary.

E-mail - In addition to the employee's obligations regarding e-mail contained in Valley Heartland CFDC *Information Security Policy*, the employee must delete all e-mail - either from internal or external sources after six (6) months. Employees will strive to keep the majority of their e-mail related to business issues. In case the e-mail needs to be referenced or retrieved, the IT department will archive e-mail upon request for six months after the employee has deleted it, after which time the e-mail will be permanently deleted. Employees will not store or transfer Valley Heartland CFDC-related e-mail on non-work-related computers. Employees will take care should they be required to send confidential/proprietary Valley Heartland CFDC information to outside sources. Any e-mail an employee deems vital to the performance of their job should be stored.

Voice mail - Voice mail is transitory in nature and may be deleted at will. There are times, however, where voice mail may require a longer retention period. For example, this may be the case where the message may be potentially used as evidence in a legal or regulatory proceeding.

Web page files—Employees will delete Web page files saved on the network or their local machines after one (1) year. This includes such pages saved from Web sites onto an employee's laptop/desktop.

Text/formatted files—Employees will conduct annual reviews of all text/formatted files (e.g., Microsoft Word documents) and will delete all those containing personal information and those they consider unnecessary or outdated. Text/formatted files the employee deems vital to the performance of his or her job should be printed and stored in the employee's workspace.

Spreadsheets—Spreadsheets other than those required to be retained by Valley Heartland CFDC for tax reasons shall be retained for approximately one (1) year or until Valley Heartland CFDC's next budget year, whichever is the earlier. Only those employees with access to Valley Heartland CFDC accounting information are permitted to delete spreadsheets.

PowerPoint presentations—All PowerPoint presentations should be deleted once they have served their useful purpose or after one (1) year whichever is the earlier.

PDF documents—Employees will delete PDF files from their network shares and/or laptops and desktops once they have served their useful purpose or after one (1) year, whichever is the earlier.

If it has been determined that an electronic document is required to be retained and it is printed or transferred to another media for longer term storage, all relevant information associated with the electronic document must also be stored. For example, header information on an e-mail would be stored in the original electronic form and should not be lost if the e-mail is printed and stored.

6.2 Compliance

Valley Heartland CFDC does not currently employ the means to automatically delete electronic files beyond the dates specified in this policy. Because of this, it is vital that employees adhere to this Policy. Each year, the Valley Heartland CFDC will choose one employee at random and check their user shares on the network and their laptops/desktop to ensure they are in compliance. Files that are beyond the designated retention date will be deleted in accordance with this policy.

7.0 Suspension of the Destruction or Disposal of Records

There are some instances where records must be held beyond the established retention period because of a complaint against an Valley Heartland CFDC Client, a privacy request, an audit, litigation, or the possibility of litigation that either does or may involve Valley Heartland CFDC.

Valley Heartland CFDC will suspend the application of a record retention schedule to a record or class of records:

- 1) Upon becoming aware of an allegation, claim, audit, investigation or pending claim, audit or investigation directed at Valley Heartland CFDC;
- 2) Where required by law or by order of a tribunal;
- 3) Where it is necessary to permit the Valley Heartland CFDC to pursue available remedies or limit any damages that it may sustain; and
- 4) Upon written notice of the commencement against a Client or employee of:
 - a) a judicial proceeding;
 - b) an administrative, regulatory or professional investigation;
 - c) a proceeding arising from an administrative, regulatory or professional investigation; or
 - d) an investigation by law enforcement or national security authorities;

The Chief Privacy Officer, or manager as directed by the Chief Privacy Officer, will create a list of records, or classes of records, for which destruction is to be suspended and attach any supporting rationale that can explain the reason for suspension. The list should provide as many details of the records to be frozen as required. Once notification of the requirement to suspend destruction or disposal is received from the Chief Privacy Officer or Manager, managers and employees will retain the affected records and suspend their destruction until appropriate notification to the contrary is received. The form of notice is found in Annex C. This notice provides a record of what has *not* been destroyed and is used as an audit trail if destruction practices are questioned. This suspension of destruction or disposal also applies to transitory records and electronic documents.

8.0 Enquiries

Any enquiries relating to the application of this policy should be directed to the Chief Privacy Officer.

Annex A Document Retention Schedule

Item/Material	Responsible Department	Storage Location	Length of Retention	Remarks	Disposal
Building Plans – Address	Executive Director	Office Administrator	Permanent.		
By-Law Amendments	Executive Director	Office Administrator	Permanent.		
Annual Reports	Executive Director	Office Administrator	Permanent.		
Items of Historical Interest	Executive Director	Office Administrator/ Store & Copy Rooms	Permanent.		
Reports of Board of Directors	Executive Director	Office Administrator	Permanent.		
Corporation Newsletter	Executive Director	Office Administrator	Current plus previous 2 years.		
Legal Cases	Executive Director	Loans Officer / Store Room	Permanent.		
Contracts	Executive Director	Office Administrator	Permanent.		
*Personnel Records (personal information) (not payroll)	Executive Director	Executive Director	10 years after termination or retirement.		Shred
Policy Letters	Executive Director	Office Administrator	Permanent.		Shred
*Dispute Documentation	Executive Director	Executive Director	Arbitration – retain for one year then retain permanently only final decision letter and signed undertakings. Mediation – retain signed undertakings.	Do not retain files of matters settled through mediation once both parties have fulfilled their obligations.	Shred
Correspondence with Lawyers	Executive Director	Office Administrator or Loans Officer	Permanent.		
CFDC Statistics for Industry Canada	Administration	Office Administrator	Year End and Year-to-Date statistics – Permanent. Quarterly Report Statistics – Current year plus previous two years.		Shred

Item/Material	Responsible Department	Storage Location	Length of Retention	Remarks	Disposal
Policy and Procedure Manuals/Handbooks	Administration	Office Administrator	Retain one copy until superseded and dispose of when no longer of reference value.		
Financial Statements - Audited & Corporation-produced	Administration	Office Administrator	Permanent.		
Facility Use Agreement	Administration	Office Administrator	Current year plus 2 years.		Shred
Budgets	Administration	Office Administrator	Current plus previous 3 years.		Shred
Special Event Registration i.e. Trade Show Exhibitors, Golf Tournament sponsors	Administration	BDSO	Current plus previous year.		Shred
Installation of Computer	Administration	Office Administrator	Until a new system is installed.		Recycle
Internet Connections Request	Administration	Office Administrator	Dispose after work is completed.		Shred
*Subscriber Agreement (ie Access to E-Learning PIN Account)	Administration	Office Administrator	Permanent, or 12 months after Corporation no longer offers this service to Clients.		Shred
*Client Records - Active - Inactive	Loans Officer	Loans Officer Store Room	All active retained. Inactive – for 7 years. Electronic records – permanent.		Shred
Un-numbered letters and memos to Clients	Administration	Office Administrator & Loans Officer	One year plus current.		Shred
Client Notice of address / name change	Administration	Office Administrator & Loans Officer	All active retained. Inactive – for 7 years.		Shred
Application for new / reinstatement: Business/Branch/Sole proprietor	Loans Officer	Loans Officer	All active retained. Inactive – for 7 years.		Shred
Client of CFDC Notice of Business Change / New Officer or Director	Loans Officer for Client Administration for CFDC	Loans Officer Office Administrator	All active retained. Inactive – for 7 years.		Shred

Item/Material	Responsible Department	Storage Location	Length of Retention	Remarks	Disposal
Application for active Client; Application for new	Loans Officer	Loans Officer	All active retained. Inactive – for 7 years.		Shred
Pension Plan/Health Plan	Administration	Office Administrator	Permanent.		
*Personnel Records (Payment Information) - Present - Previous	Administration	Office Administrator	6 years after termination or retirement.		Shred
*Financial Records	Administration	Office Administrator & Loans Officer	Current plus previous 7 years.		Shred
Emergency Contacts	Administration	Office Administrator & Executive Director	Forms for current employees only.		Shred
*Client Enrollment Registered Pension Plan – Company Name	Administration	Office Administrator	Permanent.		
Application for Group Coverage – Insurance Company Name	Administration	Office Administrator	Permanent.		
*Tax Return Information	Administration	Office Administrator	Retain current staff - former staff – dispose after 10 years.		Shred
*Financial Records - purchase orders	Administration	Office Administrator	Current plus previous 7 years.		Shred
		Administration	Current plus 2 years.		Shred
*Valley Heartland CFDC Auto Debit Service – Account Information	Loans Officer	Loans Officer	Current Clients – Permanent.		Shred
*Valley Heartland CFDC cheques (for Auto Debit to Banks)			Former Clients – within 12 months of termination.		
*Valley Heartland CFDC Auto Debit Service – credit card information					
*Non-Payment of monthly loan repayment information	Loans Officer	Loans Officer	2 years for correspondence and internal memos.		Shred
Committee Files	Administration	Office Administrator	Current plus previous 2 years.	Liaison to determine if some should be retained.	Shred
General Correspondence	All	Department	Retain 2 years, then dispose.		Shred

Item/Material	Responsible Department	Storage Location	Length of Retention	Remarks	Disposal
E-Mail Messages	Each staff	PCs	Current & previous 6 months unless filed by subject area and required for future reference.		Delete
Electronic Files				Refer also to Information Security Policy	

* Complete Annex B before destruction.

Annex B

**Valley Heartland CFDC
Certificate of Destruction**

The records identified below have been qualified for destruction:

General Description of Records

Specific Description

Record Series

Inclusive Dates (From/To)

Method of Disposal:

- Recycling;
- Shredding;
- Placement in garbage for regional landfill;
- Physically destroyed; or
- Erased in a secure manner by overwriting.

Media:

- Paper
- Magnetic tape
- Microfilm
- Optical disc

Destroyed on: _____
Date

Destroyed by:

Name _____

Signature _____

Destruction authorized by _____

Annex C
Valley Heartland CFDC
Records Destruction HOLD/RELEASE Notice

- DESTRUCTION HOLD**
Suspends destruction of all records described below until further notice

- DESTRUCTION RELEASE**
Records may be destroyed according to the established retention schedule

General Description of Records

Specific Description

Record Series

Inclusive Dates

Department Manager: _____ Date: _____

AUTHORIZATION
For Records Management Use Only

Chief Privacy Officer: _____ Date: _____

Valley Heartland Community Futures
Development Corporation

Employee Information Privacy Policy

Passed: April 20, 2004

----- Motion: B-04-034

Valley Heartland Community Futures Development Corporation

“Employee Information Privacy Policy”

1.0 Objective & Scope of Policy	1
2.0 The Collection, Use & Disclosure of Personal Information	1
3.0 Accuracy & Retention of Information	3
4.0 Security	4
5.0 Monitoring	4
6.0 Accessing and Updating Personal Information	5
7.0 What You Consent And Agree To	6
8.0 Questions	6

1.0 OBJECTIVE & SCOPE OF POLICY

This Policy Statement governs the collection, use and disclosure of Personal Information by the Valley Heartland Community Futures Development Corporation (Valley Heartland CFDC) from and about individuals who are, or seek to be, employed by Valley Heartland CFDC. It does not govern Personal Information Valley Heartland CFDC collects from and about its Members or others. It also does not cover aggregated information from which the identity of an individual cannot be determined.

This Policy Statement applies to Valley Heartland CFDC not only as an organization but also to each individual as an Employee or prospective Employee, as a condition of employment, with respect to the Personal Information of other Employees. It is to be read in conjunction with and forms part of Valley Heartland CFDC's Employee Handbook but does not rescind, replace or otherwise override any specific agreement an Employee has entered into with Valley Heartland CFDC, including any agreement concerning the confidentiality of information.

This Statement is in effect as of April 20, 2004. Valley Heartland CFDC will from time to time review and revise its privacy practices and this Policy Statement. In the event of any amendment, Employees will receive appropriate notice as soon as possible following the amendment. Policy changes will apply to the information collected from the date of the revised Policy statement as well as to existing Personal Information about Employees held by Valley Heartland CFDC.

2.0 THE COLLECTION, USE & DISCLOSURE OF PERSONAL INFORMATION

For the purposes of this Policy,

“Aggregated information” means any information, recorded in any form, about more than one individual where the identity of the individuals is not known and cannot be inferred from the information.

“Employee” means an individual currently or formerly employed by Valley Heartland CFDC in a

management or non-management capacity.

"Personal Information" means any information, recorded in any form, about an identified individual, or an individual whose identity may be inferred or determined from the information.

Valley Heartland CFDC collects and maintains different types of Personal Information from employees, including:

- (a) Identification data such as name, home address, telephone number, personal email address, date of birth, social insurance number, citizenship, and marital status;
- (b) Employment data such as salary, job title, resumes, applications, copies of school, college and university diplomas, background verification information, employment references; and
- (c) Financial information such as bank account numbers and tax related information.

Valley Heartland CFDC collects Personal Information through a variety of means and from different sources, including Personal Information that:

- Employees provide in conversations, in correspondence or through application and other forms;
- Valley Heartland CFDC receives from third parties, such as individuals or organizations who provide test results or references; and
- Employees provide using Valley Heartland CFDC's office and computer equipment and software, including e-mail and Internet applications.

Valley Heartland CFDC reserves the right to monitor employees and may collect Personal Information about employees in the course of any monitoring activities. See Section 5 for further information concerning Monitoring.

Valley Heartland CFDC uses the information provided verbally or in writing by individuals upon their application for employment (and/or which may be provided during the course of employment by Valley Heartland CFDC), for different purposes in the management and administration of the personnel relationship between Valley Heartland CFDC and that individual.

The purpose for the use (as well as the initial collection and possible disclosure) of Personal Information is for the management of the employer-employee relationship between Valley Heartland CFDC and an individual and includes, but is not limited to:

- (a) Determining eligibility for initial employment, including the verification of references and qualifications;
- (b) Administering pay and benefits;
- (c) Establishing training and/or development requirements;
- (d) Assessing qualifications for a particular job or task;
- (e) Should it be necessary, gathering evidence for disciplinary action;
- (f) Establishing a contact point in the case of an emergency (next of kin);
- (g) Complying with applicable labour or employment statutes; and

- (h) For such other purposes as required for personnel administration by Valley Heartland CFDC.

Valley Heartland CFDC's use of an Employee's Personal Information is limited to managing a person's employment by the Valley Heartland CFDC; planning and managing the Valley Heartland CFDC's personnel needs or to a purpose consistent with those purposes. Valley Heartland CFDC does not sell, trade, barter or exchange for consideration Personal Information about any Employee.

There are circumstances where the use and/or disclosure of Personal Information may be justified or permitted or where Valley Heartland CFDC is obliged to disclose information without consent. Such circumstances may include:

- Where required by law or by order of a tribunal;
- Where Valley Heartland CFDC believes, upon reasonable grounds, that it is necessary to protect the rights, privacy, safety or property of an identifiable person or group;
- Where required, to determine or administer employee pay and benefits;
- Where it is alleged that the person concerned is guilty of a criminal offence; civilly liable in a legal action or guilty of professional misconduct;
- Where it is necessary to permit the Valley Heartland CFDC to pursue available remedies or limit any damages that it may sustain; and
- Where the information is public.

Where obliged or permitted to disclose information without consent, Valley Heartland CFDC will not disclose more information than is required.

Valley Heartland CFDC may disclose Personal Information of Employees to organizations that assist the Board in the course of its fulfilling its mandate by performing services on its behalf. Personal Information will only be provided to such organizations if they agree to use such information solely for the purposes of providing services to Valley Heartland CFDC and under the instruction of Valley Heartland CFDC and, with respect to that information, to act in a manner consistent with the relevant principles articulated in this Policy Statement.

Valley Heartland CFDC will not release Personal Information about an Employee to a third party, such as a financial institution considering a loan to an Employee, beyond confirming the Employee's employment status, without the Employee's written consent. Valley Heartland CFDC will not release Personal Information about a former Employee to a potential employer, beyond confirming the former Employee's employment status, without the former Employee's written consent.

3.0 ACCURACY & RETENTION OF INFORMATION

Valley Heartland CFDC endeavours to ensure that any Personal Information of Employees in its possession is as accurate, current and complete as necessary for the purposes for which Valley Heartland CFDC uses that information.

Valley Heartland CFDC retains Personal Information about Employees as long as Valley Heartland CFDC believes it is necessary to fulfil the purpose for which it was collected. Valley Heartland CFDC has in place a *Records Retention Policy*, which outlines the procedures for the retention and subsequent disposition of Valley Heartland CFDC records including those that contain Personal Information. For example, résumés received from prospective employees that are not subsequently hired by Valley Heartland CFDC are destroyed after six months. Personal Information is retained in

An Employee's personnel file for the term of his or her employment and for ten years following such employment as required to comply with statutory or other legal purposes. Information contained in files concerning former Employees that have been closed is kept by Valley Heartland CFDC for a maximum of ten years but is not actively updated or maintained.

4.0 Security

Valley Heartland CFDC endeavours to maintain adequate physical, procedural and technical security with respect to its offices and information storage facilities so as to prevent any loss, misuse, unauthorized access, disclosure, or modification of an Employee's Personal Information.

As part of those precautions, Valley Heartland CFDC restricts access to an Employee's Personal Information to those Employees and others (i.e. individuals or organizations providing services to Valley Heartland CFDC) that it determines need to know that information in order that Valley Heartland CFDC may conduct its activities.

If any Employee misuses the Personal Information of another Employee, this will be considered as a serious offence for which disciplinary action may be taken, up to and including termination of employment, if the circumstances warrant such action. If any individual or organization misuses the Personal Information of an Employee – provided for the purpose of providing services to Valley Heartland CFDC - this will be considered a serious issue for which action may be taken, up to and including termination of the service agreement between Valley Heartland CFDC and that individual or organization, if the circumstances warrant such action.

5.0 MONITORING

Valley Heartland CFDC provides Employees with computers, telephones and related office and communication equipment as well as software applications. As is the case in other organizations, the work output of Employees, whether in paper form, computer files, or in any other form, belongs to Valley Heartland CFDC. As such, that work output, whether it is stored electronically, on paper or in any other form, and the tools used to generate that work product are always subject to review by Valley Heartland CFDC.

In the course of performing its mandate, Valley Heartland CFDC may monitor Employee activities and its property. To illustrate what monitoring means, Employee e-mail In-boxes will normally contain the e-mails they have sent and received. Back-ups and archives may also contain copies of e-mails that Employees have deleted. The e-mail system is Valley Heartland CFDC property and Employees may send and receive personal e-mail on the understanding that such e-mail is not private or confidential. Valley Heartland CFDC reserves the right to monitor the e-mail system, whether the mail is sent/received/created regardless of whether a personal access code is used. The actual content of messages, the date and time the message was transmitted, received and opened and the e-mail addresses of the sender and recipients will normally be recorded for the benefit of Valley Heartland CFDC.

With web browsing the URLs (Uniform Resource Locaters or website addresses) of sites visited, the date and time they were visited and the duration of site visits may be logged. Normally, access rights to staff mail boxes and logs would be restricted to those with the responsibility for administering the system.

Valley Heartland CFDC will monitor its computer resources to ensure that damage to or illegal use of those resources is limited (e.g. by viruses or Trojan horses). It may monitor the physical premises to ensure that only authorized personnel access Valley Heartland CFDC offices or certain areas within Valley Heartland CFDC offices. It does these things so as to ensure the efficient use of its systems and equipment, to protect Valley Heartland CFDC property and to ensure compliance with applicable laws and Valley Heartland CFDC policies. Access rights to Employee mail boxes and logs will be restricted to those with the responsibility for administering Valley Heartland CFDC's Information Technology systems. Such access will be as limited as possible.

This section is not meant to suggest that Employees will be monitored or their actions subject to constant surveillance. It is meant to bring to attention the fact that such monitoring may occur and may result in the collection of Personal Information from Employees (e.g. through their use of Valley Heartland CFDC's resources). ***When using Valley Heartland CFDC equipment or resources Employees should not have any expectation of privacy with respect to their use of such equipment or resources.*** Any collection of Personal Information held or used in the course of monitoring will not be more than is necessary for the purpose of the monitoring.

Monitoring is or will be done on an "as required" basis and will be in proportion to the risks that Valley Heartland CFDC faces. Valley Heartland CFDC will conduct any monitoring in the least intrusive way possible. In some instances, Valley Heartland CFDC may supplement this monitoring notice with more specific ones, as appropriate.

6.0 ACCESSING AND UPDATING PERSONAL INFORMATION

Valley Heartland CFDC permits the reasonable right of access and review of Personal Information about an Employee held by the Board. If an Employee believes the information about them is not correct, the Employee may request an update of that information by making a request to the Executive Director. Valley Heartland CFDC reserves the right not to change any Personal Information but will append any alternative text the individual concerned believes appropriate.

Where information will be disclosed, Valley Heartland CFDC will endeavor to provide the information in question within a reasonable time and no later than 60 days following the request. Valley Heartland CFDC may charge a minimal or nominal cost (e.g. photocopying, mail charges) to the individual making the request.

To guard against fraudulent requests for access, Valley Heartland CFDC will require sufficient information to allow it to confirm that the person making the request is authorized to do so before granting access or making corrections. This may occur, for example, in the case of an authorized representative seeking information about a former or deceased Employee or where law enforcement authorities seek information about an Employee.

Valley Heartland CFDC reserves the right to decline to provide access to Personal Information where the information requested:

1. Would disclose:
 - a. The Personal Information of another individual or of a deceased individual; or
 - b. Trade secrets or other business confidential information that may harm Valley Heartland CFDC or competitive position of a third party or interfere with contractual or other negotiations of Valley Heartland CFDC or a third party;

2. Is subject to solicitor-client or litigation privilege;
3. Is not readily retrievable and the burden or cost of providing would be disproportionate to the nature or value of the information;
4. Does not exist, is not held, or cannot be found by Valley Heartland CFDC;
5. Could reasonably result in serious harm to the treatment or recovery of the individual concerned, serious emotional harm to the individual or another individual, or serious bodily harm to another individual; or
6. May harm or interfere with law enforcement activities and other investigative or regulatory functions of a body authorized by statute to perform such functions.

Where information will not or cannot be disclosed, the individual making the request will be provided with the reasons for non-disclosure.

Valley Heartland CFDC will not respond to repetitious or vexatious requests for access. In determining whether a request is repetitious or vexatious, the Board will consider such factors as the frequency with which information is updated, the purpose for which the information is used, and the nature of the information.

7.0 WHAT YOU CONSENT AND AGREE TO

When an Employee provides Valley Heartland CFDC with Personal Information, that Employee *consents to the collection, use and possible disclosure of Personal Information about that individual as described in Section 2 above; and agrees to the terms for accessing and correcting data as described in Section 6 above.*

8.0 QUESTIONS

In the event an Employee has questions about (a) access to Personal Information; (b) the collection, use, management or disclosure of Personal Information, or (c) this Policy Statement or whether Valley Heartland CFDC is acting in a manner consistent with it, that Employee should contact the Chief Privacy Officer.



VALLEY HEARTLAND

Community Futures Development Corporation

Notice to clients about our compliance with the Federal Privacy Law

On January 1, 2004, the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") came into effect for all businesses and non-profit organizations such as Valley Heartland Community Futures Development Corporation that collect, use, retain and disclose personal information obtained from its clients in the course of its commercial activities.

In recognition of the significance and necessity of confidentiality in personal and business information, Valley Heartland Community Futures Development Corporation has always taken steps to safeguard your information from unauthorized access and disclosure. In that respect, when you applied for a business loan or loan guarantee, you provided consent to Valley Heartland Community Futures Development Corporation to retain and disclose personal information about you for the purposes set out in the application, subject to applicable Federal and Provincial laws.

With the coming into force of *PIPEDA*, Valley Heartland Community Futures Development Corporation has taken further steps to ensure your personal and business information is handled in accordance with this Federal privacy legislation. Included with this notice is a copy of Valley Heartland Community Futures Development Corporation's Privacy Statement, which statement summarizes our Privacy Policy and policies and procedures governing information security, record retention and destruction.

Subject to applicable laws and with specific exceptions to protect the privacy of third parties, clients may access their personal information held by Valley Heartland Community Futures Development Corporation by submitting a request for access, in writing, to Valley Heartland Community Futures Development Corporation's Chief Privacy Officer. Any corrections to such information will be made, if required, in accordance with the Valley Heartland Community Futures Development Corporation Privacy Policy.

A copy of Valley Heartland Community Futures Development Corporation's Privacy Policy, is available at our web site at www.valleycfdc.com can be provided by contacting the Valley Heartland Community Futures Development Corporation's Chief Privacy Officer at 613-283-7002.



VALLEY HEARTLAND

Community Futures Development Corporation

Client Consent to Disclose Information to Third Party

I, _____, give Valley Heartland Community Futures Development Corporation permission to disclose my personal information to the following third party service providers:

- [Name of Financial Institution]
- [Credit Bureau of Canada]
- [Name of Insurance consultant/provider]
-

The use of my personal information by the above providers is limited to the administration of the services as prescribed by Valley Heartland Community Futures Development Corporation and cannot be used for any other purposes.

The information provided to these companies includes the following:

- Name, address, phone number, date of birth, gender;
- Social Insurance Number (optional);
- Job title, Employer;

All personal information changes are to be reported to _____ at Valley Heartland and, in turn, these changes will be reported to the above-listed service providers.

Signature

Date



VALLEY HEARTLAND

Community Futures Development Corporation

CONFIDENTIALITY AGREEMENT FOR EMPLOYEES AND VOLUNTEERS

To: Valley Heartland Community Futures Development Corporation

I, _____, the undersigned understand the significance and necessity of confidentiality of personal and business information arising from the business affairs and activities of Valley Heartland Community Futures Development Corporation. I, therefore, covenant and agree to keep any information received in the course of my duties, office, role or capacity with Valley Heartland Community Futures Development Corporation strictly confidential.

I confirm receipt of the Privacy Policy for Valley Heartland Community Futures Development Corporation and pledge that I will comply with the said Privacy Policy respecting any and all information received or learned by me about all bodies, businesses, individuals and subjects during the course of my duties, office, role or capacity with Valley Heartland Community Futures Development Corporation.

I also confirm receipt of Valley Heartland Community Futures Development Corporation *Employee Information Privacy Policy*, and Valley Heartland Community Futures Development Corporation *Information Security, Retention and Destruction Policy* and will handle, retain and dispose of personal and business information in electronic and hard copy formats in accordance with these policies.

I further covenant and agree to take all steps necessary to preserve the confidential nature of personal and business information learned or received by me in the course of my duties, office, role or capacity with Valley Heartland Community Futures Development Corporation in accordance with the aforementioned privacy policies in the event that I leave this position with Valley Heartland Community Futures Development Corporation.

I understand that a breach of this confidentiality agreement will be brought to the attention of the Executive Committee of the Board of Directors and I may be subject to discretionary disciplinary action and possible termination of employment or volunteer appointment on Valley Heartland Community Futures Development Corporation committee and/or Board of Directors.

Signature

Print Name

Witness

Date



VALLEY HEARTLAND

Community Futures Development Corporation

THIRD-PARTY CONFIDENTIALITY AGREEMENT ¹

THIS AGREEMENT, made this _____ day of _____, 202_, between:

Valley Heartland Community Futures Development Corporation (the "Corporation")

- and -

[Name of Company or Individual] (the "Recipient")

RECITES THAT:

- (a) On and subject to the terms and conditions of this Agreement, the Corporation intends to disclose certain personal information to the Recipient for purposes of the Activity whose terms are defined in this Agreement.

THEREFORE, in return for the promises and mutual agreements contained in this agreement and other good and valuable consideration (the receipt and sufficiency of which is acknowledged by each of the Parties), the Parties agree as follows:

1. **DEFINITIONS.** In this Agreement, unless the context otherwise requires:

"Activity" means [to be defined at the time of preparing the Third Party Confidentiality Agreement, *for example - the provision of office cleaning services for which the Corporation has contracted with the Recipient*];

"Agreement" means this contract to safeguard personal and business information and any document signed by the Corporation and the Recipient amending this agreement;

"Business Information" means any information that is used by an individual with regards to the operation or promotion of his or her business;

"Personal Information" means any information about an identifiable individual provided by an individual or business applicant or client of the Corporation to the Recipient, or that becomes known to the Recipient in the course of his or her activity on behalf of the individual or business as contracted to provide with the Corporation;

¹ To be signed by all third party service providers or third party recipients of Personal Information respecting the Corporation's clients and employees and Business Information.

"Processing" means any manual, automated, or electronic, form of collection, use, transmission, disclosure, storage, reproduction, manipulation, modification, or access to the Personal Information and Business Information defined within this agreement.

"Safeguards" means any method or combination of methods that have been agreed to between the Corporation and the Recipient to protect the personal information or business information from loss or theft, as well as unauthorized access, disclosure, copying, use or modification of personal information or business information.

2. SAFEGUARDS TO BE APPLIED

The Recipient acknowledges and confirms that personal information and business information is being disclosed to the Recipient for the purposes of the activity only. Accordingly, the Recipient agrees to:

- (a) exercise all reasonable precautions to protect the personal information and business information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification;
- (b) use the personal information and business information for the purposes of the activity only;
- (c) not use the personal information and business information for its own benefit or the benefit of third parties;
- (d) not disclose the personal information and business information, or the knowledge of its existence and use by the Recipient, to any Third Party;
- (e) cease any and all use of the personal information and business information, and return the said information to the Corporation or destroy the said information in accordance with the Corporation's *Information Security, Retention and Destruction Policy*, upon request of the Corporation; and
- (f) permit site visits by the Corporation to examine the measures taken by the Recipient to protect the personal information and business information, upon reasonable notice.

3. BEGINNING AND EXPIRY OF THE RECIPIENT'S OBLIGATIONS

The Recipient's obligations under this agreement take effect as of the date of this agreement and survive until [number of days, months, years] from that date, the completion of the activity, or the Corporation's request for a return of the personal information and business information, whichever comes last.

4. ACKNOWLEDGEMENTS

The Recipient acknowledges that it is aware of the Corporation's privacy policies and procedures. The Recipient agrees to immediately implement appropriate technical and organizational safeguards and procedures in a manner that is consistent with these principles and policies to protect any personal information and business information to which it may have access in connection with this agreement. The Recipient will not collect, use, disclose or transfer personal information and business information without prior written instructions from the Corporation.

The Recipient also acknowledges that it is aware of all applicable Canadian laws regarding the protection of personal information collected, used, disclosed or transferred in connection with commercial activities. The Recipient shall comply, and shall cause all representatives of the Recipient to comply, with all such applicable laws.

5. INDEMNITY

The Recipient indemnifies and holds the Corporation harmless from and against any and all loss, liability, damage, claim, cost, and expense (including legal fees) however arising, out of any breach or non-performance by the Recipient or its representatives of any of the Recipient's obligations under this agreement including, without limitation, the Recipient's obligations regarding the use of personal information and business information.

6. INJUNCTION

The Recipient acknowledges that a breach by it or any of its representatives of any of the Recipient's obligations under this agreement may cause irreparable harm to the Corporation which may be difficult or impossible to ascertain, and that an award of damages will not be a sufficient remedy for such breach. Accordingly, the Corporation will be entitled to specific performance of this agreement and an injunction to prevent any breach or threatened breach of this agreement. No remedy referred to in this section is exclusive by each is cumulative and in addition to any other remedy otherwise available at law or in equity, including damages.

7. GENERAL

- (a) Nothing in this agreement is to be interpreted to:
 - (i) obligate the Corporation to enter into any further agreement with the Recipient; or
 - (ii) grant to the Recipient any right, title, or interest in the Personal Information or Business Information, or in the Corporation's operations.
- (b) Any communication under this agreement is deemed to have been properly made when, in the ordinary course of delivery or transmission, it is sent to the Recipient at its address above or other address as the Recipient advises, in writing.
- (c) Notwithstanding any dispute arising between the Corporation and the Recipient, the Recipient must proceed diligently with the performance of this agreement.
- (d) No delay or failure of the Corporation or the Recipient to exercise any of its rights under this agreement operates as a waiver of such right or affects any other of the Corporation's or the Recipient's rights or the exercise of those rights.
- (e) This Agreement benefits and is binding on the Corporation and the Recipient, as well as their respective heirs, executors, administrators, successors, and permitted assigns, as the case may be.
- (f) This Agreement is governed by and must be construed in accordance with the laws of the province of Ontario, and the law of Canada, as applicable in Ontario, and the Corporation and the Recipient irrevocably submit to the exclusive jurisdiction of the courts of Ontario for interpretation and enforcement of this agreement.

- (g) If any term of this agreement is held to be invalid, illegal, or unenforceable, it will not affect the validity of any other terms of this agreement and this agreement will be read as though the invalid term does not exist.
- (h) The Recipient agrees not to assign this agreement or any of its rights, obligations, or interests under this agreement without the prior written consent of the Corporation. Notwithstanding such consent, no assignment relieves the Recipient of any of its obligations under this agreement.
- (i) This agreement expresses the final agreement between the Corporation and the Recipient as to the subject matter of this agreement. Accordingly, the Corporation and the Recipient agree not to amend this agreement except by and in accordance with a document signed by the both parties.

EACH OF THE PARTIES have executed this agreement and in so doing confirm their authority and intention to bind the party they represent.

SIGNED at _____, this _____ day of _____, 202__.

the Corporation

By: _____

Name: _____

Title: _____

THE RECIPIENT [NAME OF COMPANY/PERSON]

By: _____

Name: _____

Title: _____



VALLEY HEARTLAND

Community Futures Development Corporation

Client Consent to Disclose Information to Third Party

I, _____, give Valley Heartland Community Futures Development Corporation permission to disclose my personal information to the following third party service providers:

- [Name of Financial Institution]
- [Credit Bureau of Canada]
- [Name of Insurance consultant/provider]
-

The use of my personal information by the above providers is limited to the administration of the services as prescribed by Valley Heartland Community Futures Development Corporation and cannot be used for any other purposes.

The information provided to these companies includes the following:

- Name, address, phone number, date of birth, gender;
- Social Insurance Number (optional);
- Job title, Employer;

All personal information changes are to be reported to _____ at Valley Heartland and, in turn, these changes will be reported to the above-listed service providers.

Signature

Date



VALLEY HEARTLAND

Community Futures Development Corporation

I, _____, give Valley Heartland CFDC permission to disclose my personal information to the following third party service providers:

- Desjardins Financial Security [Health Benefits consultant/provider]
- Standard Life Assurance Company [Group RRSP consultant/provider]

The use of my personal information by the above providers is limited to the administration of the services as prescribed by Valley Heartland CFDC and cannot be used for any other purposes.

The information provided to these companies includes the following:

- Name, address, phone number, date of birth, gender;
- Social Insurance Number;
- Salary, job title, employment start date;
- Name, gender, and date of birth of all eligible dependants I require benefit coverage for, or name as a beneficiary.

All personal information changes are to be reported to Sharen Symondson at Valley Heartland CFDC and, in turn, these changes will be reported to the above-listed service providers.

Signature

Date

Valley Heartland CFDC

Complaint Policy

Valley Heartland CFDC is committed to providing excellence in customer service to its clients and recognizes the value of complaints as an important tool in monitoring client satisfaction.

Policy

1. All client complaints shall be dealt with in a professional and timely manner. Valley Heartland CFDC will work with the Complainant to establish a resolution that is fair and accurately reflects Valley Heartland's Vision and Mission.
2. For the purposes of this policy the client shall include any individual seeking or engaging the services of Valley Heartland CFDC.

Procedure

1. Any complaints shall be taken seriously and the staff will strive for resolution through discussion with the Complainant at the time of the issue.
2. Formal complaints shall be registered in writing through a Complaints Form. Personal data collected on the Complaints Form will be handled according to Valley Heartland CFDC's privacy policy.
3. The Executive Director or designate will ensure that all complaints are acknowledged by e-mail or other written form within 10 business days of receipt of complaint.
4. A response to the Complainant shall be made in writing within 30 business days of receiving the complaint.
5. Valley Heartland CFDC will make every reasonable effort to investigate the complaint. It will liaise with staff members and any other relevant parties to investigate the complaint and ensure a satisfactory outcome for the Complainant. A record of all information relating to the investigation will be kept in a secure file in the Executive Director's office.
6. Following an appropriate investigation, the Executive Director will advise the Complainant in writing of the action or decision taken in regards to the complaint. A copy of this decision will also be kept in a secure file.
7. If not satisfied with the response, the Complainant may make appeal in writing to Valley Heartland CFDC's Board of Directors for review of the Executive Director's decision. The decision of the Board will be provided to the Complainant in writing within 30 days of receipt of the appeal. The Board's decision will be considered final.

Valley Heartland Internal & External Communication Policy

The purpose of this policy is to preserve the professional image of Valley Heartland Community Futures Development Corporation externally and to promote a team approach to the conduct of the business of Valley Heartland Community Futures Development Corporation amongst and between Board members, employees and resource members.

NOTE: Reference to Board members and employees in the following policy are intended to refer to all members of the Board of Directors; all officers of the Board, specifically the Chairperson, Vice-Chairperson, Secretary and Treasurer; and all employees of Valley Heartland Community Futures Development Corporation.

Board members and employees agree to:

1. Promote the programs of Valley Heartland Community Futures Development Corporation.
2. Support the decisions of the Board of Directors made in accordance with the by-laws of Valley Heartland Community Futures Development Corporation.
3. Respect the inability of an employee or Board member to exercise individual authority when interacting with the public, the press, other entities, employees, Board members or the Chairperson except when acting at a meeting the Board of Directors or as a delegate of the Board of Directors, authorized by the Board to do so.
4. Recognize the Chairperson or the Executive Director as the primary spokesperson for Valley Heartland Community Futures Development Corporation.
5. Recognize the Vice-Chairperson or the General Manager as the spokesperson for Valley Heartland Community Futures Development Corporation in the absence of the Chairperson.
6. Refer all external inquiries regarding the official business of Valley Heartland Community Futures Development Corporation to the Chairperson and/or the General Manager.
7. Contact the Chairperson and the General Manager to pose questions, address concerns and/or make suggestions between Board meetings.
8. Advise the Chairperson and General Manager of any activities that arise that could result in litigation against Valley Heartland Community Futures Development Corporation.
9. Advise the Chairperson and General Manager of any occurrences the Board members or the Executive Director would hear about through another public channel.
10. Advise the Chairperson and General Manager of instances where someone may file a complaint to a Board member, Officer, Chairperson or employee.
11. Deal with issues immediately, candidly and openly.

The Chairperson and General Manager specifically agree to:

1. Keep all Board members apprised of situations and developments that could have an impact on the overall organization.



2. Advise all Board members, in a timely manner, of any occurrences that the Board members would hear about through another public channel.
3. Respond to every media question while refraining from volunteering negative information.
4. Refrain from speaking off the record about Valley Heartland Community Futures Development Corporations activity.

This policy is to be reviewed annually by the Board of Directors and employees and revised as necessary.

