CONESTOGA FUNDS

POLICIES AND PROCEDURES
ON PRIVACY OF CUSTOMER INFORMATION
AND DISPOSING OF CONSUMER REPORT INFORMATION

ESTABLISHMENT AND PURPOSE

The Board of Trustees of Conestoga Funds (the "Trust"), on behalf of the Small, SMid Cap Funds and LargeCap Fund (the "Funds"), hereby establishes these policies and procedures (the "Policy") regarding the privacy of the records and information of the Fund's customers ("Customer Information"). The purpose of the Policy is to address administrative, technical, and physical safeguards for the protection of Customer Information. The Policy is reasonably designed to:

1. Insure the security and confidentiality of Customer Information;

2. Protect against any anticipated threats or hazards to the security or integrity of Customer Information; and

3. Protect against unauthorized access to or use of Customer Information that could result in substantial harm or inconvenience to any customer.

The term "customer" has the same meaning as set forth in Rule 3(j) of Regulation S-P under the Gramm-Leach-Bliley Act. The term "Customer Information" has the same meaning as the term "nonpublic personal information" as set forth in Rule 3(t) or Regulation S-P.

In addition, Regulation S-P, in accordance with the Fair and Accurate Credit Transactions Act of 2003, requires the Trusts to properly dispose of consumer report information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal. In defining "consumer report information," Regulation S-P refers to Section 603(d) of the Fair Credit Reporting Act (the "FCRA"), which defines the term as ". . . any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under section 604 [of the FRCA]."

PRIVACY POLICY

In accordance with Regulation S-P, the Trust has adopted a policy with respect to the treatment of Customer Information, a copy of which is attached to this Policy as Exhibit A.

DELEGATION TO SERVICE PROVIDERS

Customer records and information are maintained on the Trust's behalf by Conestoga Capital Advisors, LLC, Small and SMid Cap Fund's investment adviser and Institutional Advisors, LLC, LargeCap Fund's investment adviser (the "Advisers"), and by Mutual Shareholder Services, LLC, the Funds' transfer agent (the "Transfer Agent"). Accordingly, the Trust has delegated to these entities the responsibility of safeguarding Customer Information and disposing of consumer report information appropriately. The relevant policies and procedures of the Advisers and the Transfer Agent are attached to the Policy as Exhibits B, C, and D respectively.
These entities may amend these policies from time to time, without Board approval, and such amended policies shall be attached to the Policy as exhibits.

OVERSIGHT BY THE BOARD

A. Review by Chief Compliance Officer ("CCO")

The CCO shall review the adequacy and effectiveness of the Policy at least annually and recommend changes, if any, to the Board.

B. Review by the Board

The Board shall review the adequacy and effectiveness of the Policy at least annually and consider any recommendations, if any, of the CCO.

Adopted: July 1, 2005
Ratified by the Board: August 18, 2005
Revised: January 21, 2014

Exhibit A

Conestoga Funds Privacy Policy

This notice is being provided to you in accordance with the Securities and Exchange Commission's rule regarding the privacy of consumer financial information ("Regulation S-P"). Please take the time to read and understand the privacy policies and procedures that we have implemented to safeguard your nonpublic personal information.[1]

Information We Collect

The Conestoga Funds must collect certain personally identifiable financial information about its customers to ensure that it offers the highest quality financial services and products.

The personally identifiable financial information which we gather during the normal course of doing business with you may include:

- information we receive from you on applications or other forms;

- information about your transactions with us, our affiliates, or others;

- information collected through an Internet "cookie" (an information collecting device from a web server); and

- information we receive from a consumer reporting agency.

Information We Disclose

We do not disclose any nonpublic personal information about our customers or former customers to anyone, except as permitted by law. In accordance with Section 248.13 of Regulation S-P, we may disclose all of the information we collect, as described above, to certain nonaffiliated third parties such as attorneys, accountants, auditors and persons or entities that are assessing our compliance with industry standards. We enter into contractual agreements with all nonaffiliated third parties that prohibit such third parties from disclosing or using the information other than to carry out the purposes for which we disclose the information.

Confidentiality and Security

We restrict access to nonpublic personal information about you to those employees who need to know that information to provide financial products or services to you. We maintain physical, electronic, and procedural safeguards that comply with federal standards to guard your nonpublic personal information.

[1] Nonpublic personal information means personally identifiable financial information and any list, description, or other grouping of consumers that is derived using any personally identifiable financial information that is not publicly available.

Exhibit B

CONESTOGA CAPITAL ADVISORS, LLC
Policy

Issue

The SEC's Regulation S-P (Privacy of Consumer Financial Information), which was adopted to comply with Section 504 of the Gramm-Leach-Bliley Act, requires investment advisers to disclose to clients its policies and procedures regarding the use and safekeeping of personal information.

Personal information is collected from clients at the inception of their accounts and occasionally thereafter, primarily to determine accounts' investment objectives and financial goals and to assist in providing clients with a high level of service.

While CCA strives to keep client information up to date, clients are requested to monitor any information provided to them for errors.

Policy

CCA will not disclose a client's personal information to anyone unless it is permitted or required by law, at the direction of a client, or is necessary to provide CCA's services.

Procedures

1. CCA shall not sell client information to anyone.

2. CCA will restrict access to clients' personal information to individuals within CCA who require the information in the ordinary course of servicing clients' accounts. Client information is used only for business purposes.

3. CCA has developed procedures to safeguard client records and information (See Attachment A).

4. Client information may only be given to third-parties under the following circumstances:
- To broker/dealers to open a client's brokerage account;
- To other firms as directed by clients, such as accountants, lawyers, etc.;
- To specified family members; and
- To regulators, when required by law.

5. At times, client information may be reviewed by CCA's outside service providers (i.e. – accountants, lawyers, consultants, etc.). CCA will review the entities' privacy policies to ensure that clients' information is not misappropriated or used in a manner that is contrary to CCA's privacy policies.

6. CCA shall provide a privacy notice (See Attachment B) to clients (i.e. "natural persons") upon inception of the relationship and annually thereafter. CCA will maintain a record of the dates when the privacy notice is provided to clients.

7. In the event of a change in the privacy policy, CCA will provide its clients with a sufficient amount of time to opt out of any disclosure provisions.

8. Any suspected breaches to the privacy policy should be reported to the CCO and/or another partner.

9. If an employee receives a complaint regarding a potential identity theft issue (be it from a client or other party), the employee should immediately notify the CCO. The CCO will thoroughly investigate any valid complaint, and maintain a log of all complaints as well as the result of any investigations.

10. In the event that unintended parties receive access to personal and confidential information of California residents, CCA will disclose those clients of the privacy breech. See Senate Bill No. 1386.

Responsibilities

The CCO will monitor for compliance with CCA's Privacy Policy and Name will coordinate the dissemination of the Privacy Notice.

Attachment A

1. Procedures to Safeguard Client Records and Information

CCA shall (a) ensure the security and confidentiality of consumer, customer and former customer records and information; (b) protect against any anticipated threats or hazards to the security or integrity of consumer, customer and former customer records and information; and (c) protect against unauthorized access to or use of consumer or customer records or information that could result in substantial harm or inconvenience to any customer. Accordingly, the following procedures will be followed:

A. **Desktop Computer Security Guidelines**.

1. Definition

Desktop computers are personal workstations that, though possibly linked to other computers via a Local Area Network, function as stand-alone units.

2. Hardware Security

a) Lock main office. The office keys should be monitored to ensure they are returned when an employee leaves CCA.
b) Locate computers away from environmental hazards.
c) Follow standard data backup procedures.

3. Access Security

a) Utilize password facilities to ensure that only authorized users can access the system. Where the Desktop is located in an open space or is otherwise difficult to physically secure, consideration should be given to enhanced password protection mechanisms and procedures.
b) Password guidelines:
- Length should be eight characters. (Six-character passwords may suffice for non-dictionary words.)
- Avoid words found in the dictionary and include at least one numeric character.
- Choose passwords not easily guessed by someone acquainted with the user. (Passwords should not be maiden names, or names of children, spouses, or pets.)
- Do not write passwords down anywhere.
- Change passwords periodically.
- Do not include passwords in any electronic mail message.

4. Data and Software Availability

a) Back up and store important records and programs on a regular schedule.

b) Check data and software integrity.
c) Fix software problems immediately.

5. Confidential Information

a) Encrypt sensitive and confidential information where appropriate.
b) Monitor printers used to produce sensitive and confidential information.
c) Overwrite sensitive files on floppy disks and CDs.

6. Viruses

Computer viruses are self-propagating programs that infect other programs. Viruses and worms may destroy programs and data as well as using the computer's memory and processing power. Viruses, worms, and Trojan horses are of particular concern in networked and shared resource environments because the possible damage they can cause is greatly increased. Some of these cause damage by exploiting holes in system software. Fixes to infected software should be made as soon as a problem is found.

To decrease the risk of viruses and limit their spread:

a) Check all software before installing it.
b) Use software tools to detect and remove viruses.
c) Isolate immediately any contaminated system.

7. Computer Networks

Networked computers may require more stringent security than stand-alone computers because they are access points to computer networks. While CCA has the responsibility for setting up and maintaining appropriate security procedures on the network, each individual is responsible for operating their own computer with ethical regard for others in the shared environment. The following considerations and procedures must be emphasized in a network environment:

a) Check all files downloaded from the Internet. Avoid downloading shareware files.
b) Test all software before it is installed to make sure it doesn't contain a virus/worm that could have serious consequences for other personal computers and servers on the Firm network.
c) Choose passwords with great care to prevent unauthorized use of files on networks or other personal computers.
d) Always BACK-UP your important files.
e) Use (where appropriate) encrypting/decrypting and authentication services to send confidential information over the Internet.

B. **Physical Data Security Guidelines**

1. During working hours, authorized personnel must occupy the area where we maintain or regularly use nonpublic client information or restrict storage of such information to locked metal file cabinets or a locked room. During nonworking hours, nonpublic personal information should be stored in a locked room. Where the locked room is the system of security, no master key should be available. A master key opens rooms other than the room containing the nonpublic personal information. Where the locked room contains records accessible by unauthorized individuals, separate the records into individual locked file cabinets.

2. If your duties require handling nonpublic personal information, you must always take care to protect the integrity, security, and confidentiality of these records. Do not put papers containing nonpublic personal information into the recycle bins or trash receptacles (e.g., client lists, account statements, tax returns). Confidential material should be shredded.

C. **Identity Theft**

1. An identity thief can obtain a victim's personal information through a variety of methods. Some of these methods are directly related to CCA and industry practices that put consumers at risk. Employees should be aware of how their actions may expose our clients to the dangers of identity theft.

2. Employees should take the following actions to prevent identity theft:

a) When providing copies of information to others, employees should make sure that nonessential information is removed and that nonpublic personal information that has no relevance to the transaction is either removed or masked.

b) The practice of *dumpster diving* provides access for a would-be thief to a client's personal information. If you discard papers containing personal client identification information without shredding the documents, a thief may retrieve this information from our waste management facilities. Therefore, when disposing of paper documents, the papers should be shredded.

c) To help prevent a fraudulent address change, verify requests before executing them. Send confirmation of address changes to both the new and the old address of record.

d) CCA's employees may also be deceived by *pretext calling*, defined as an information broker or identity thief calling CCA while pretending to be a client, and may even use bits of a client's personal information (such as a Social Security Number) to maintain the deception. The information thief convinces the employee to provide additional information over the phone,

which can be used for fraudulent purposes. Employees should make absolutely certain that they confirm the identity of the client on the phone before divulging personal information.

e) CCA prohibits the display of Social Security Numbers on any documents that are widely seen by others (e.g. client files, mailing lists, quarterly reports, etc.).

f) Employees may be responsible for identity theft through more direct means. Insider access to information allows a dishonest employee to sell consumers' personal information or to use it for fraudulent purposes. Such action is cause for immediate termination of employment and may subject the employee to civil and criminal liability.

Attachment B

2. Privacy Notice

This notice is being provided to you in accordance with the Securities and Exchange Commission's rule regarding the privacy of consumer financial information ("Regulation S-P"). Please take the time to read and understand the privacy policies and procedures that we have implemented to safeguard your nonpublic personal information.[1]

INFORMATION WE COLLECT

Conestoga Capital Advisors, LLC must collect certain personally identifiable financial information about its customers to ensure that it offers the highest quality financial services and products. The personally identifiable financial information which we gather during the normal course of doing business with you may include:

1. information we receive from you on applications or other forms;

2. information about your transactions with us, our affiliates, or others;

3. information collected through an Internet "cookie" (an information collecting device from a web server); and

4. information we receive from a consumer reporting agency.

INFORMATION WE DISCLOSE

We do not disclose any nonpublic personal information about our customers or former customers to anyone, except as permitted by law. In accordance with Section 248.13 of Regulation S-P, we may disclose all of the information we collect, as described above, to certain nonaffiliated third parties such as attorneys, accountants, auditors and persons or entities that are assessing our compliance with industry standards. We enter into contractual agreements with all nonaffiliated third parties that prohibit such third parties from disclosing or using the information other than to carry out the purposes for which we disclose the information.

CONFIDENTIALITY AND SECURITY

We restrict access to nonpublic personal information about you to those employees who need to know that information to provide financial products or services to you. We maintain physical, electronic, and procedural safeguards that comply with federal standards to guard your nonpublic personal information.

[1] Nonpublic personal information means personally identifiable financial information and any list, description or other grouping of consumers that is derived using any personally identifiable financial information that is not publicly available.

Exhibit B

Institutional Advisors, LLC
Privacy Policy

Privacy Notice
This notice is provided by the following companies within the National Penn family.
National Penn Bancshares, Inc.

Subsidiaries: National Penn Bank
National Penn Investment Company
Christiana OREO LLC

National Penn Bank

Divisions: Hometowne Heritage Bank
Nittany Bank
KNBT

Subsidiaries: National Penn Wealth Management, N.A.
Division – National Penn Investors Trust Company
National Penn Capital Advisors Inc.
Division – Resources for Retirement Inc.
National Penn Insurance Services Group Inc.
Division – Higgins Insurance
Subsidiary – Caruso Benefits Group Inc.
Institutional Advisors LLC
National Penn Management Services, LLC
DFM Realty, Inc.
Link Financial Services Inc.
Division – Link Abstract, L.P.
NPB Delaware, Inc.
KNBT Settlement Services LLC
National Penn Leasing Company
Laurel Abstract Company

*Your account may be with an insurance company that is serviced through National Penn Insurance Agency.

In order to ensure that everyone receives a copy of this customer privacy notice as required, you may receive more than one copy. Thank you for choosing National Penn. If you have questions or would like more information, please call our customer service center at 1.800.822.3321 or visit us online at www.natpennbank.com.

OUR COMMMITMENT TO YOU

National Penn Bancshares, Inc. (“National Penn”) is committed to providing you and your family with financial products and services to meet your needs and your family’s financial goals. We recognize that your relationship with us is based on trust, and that you expect us to act responsibly and in your best interests. Because we respect that your personal and financial data is your private information, we hold ourselves to high standards in its safekeeping and use.

We want you to know that we do not sell customer information. Instead, your information is used by us primarily to complete transactions that you request or to make you aware of other financial products and services that we would like to offer you.

The purpose of this notice is to explain how we collect, use and safeguard your personal financial information.

You may have other privacy protections under state laws. We will comply with them with regard to our information practices.

INFORMATION WE COLLECT ABOUT YOU

We may collect "nonpublic personal information" about you from the following sources:

- Information we receive from you on applications or other loan and account forms, such as your name, address, social security number, assets and income;
- Information about your transactions with us, our affiliates or others, such as your account balance, payment history, parties to transactions and credit card usage;
- Information we receive from credit reporting agencies, such as your creditworthiness and credit history; and
- Information we receive from your internet usage when you visit our web sites.

“Nonpublic personal information” is nonpublic information about you that we obtain in connection with providing a financial product or service to you. For example, nonpublic personal information includes information regarding your account balance, payment history and overdraft history.

In this privacy notice, the words “you” and “customer” are used to mean any individual who obtains or has obtained a product or service from National Penn that is to be used primarily for personal, family or household purposes.

This notice also applies to former customers, and to consumers who have provided information to us but have not entered into a customer relationship, for as long as information is retained.

INFORMATION WE MAY DISCLOSE

- To Service Your Accounts

To assist us in providing products/services you have requested, we may disclose information we collect about you, as described above, to our affiliates and third party financial service providers.

Such information may be shared for purposes including mortgage and account servicing, and payment and data processing services.

- To Provide Information About Products/Services

To provide you with information regarding financial, insurance, investment and other products/services that may be of interest to you, we may disclose information we collect about you, as described above, to our affiliates and third parties. These companies may be financial service providers (such as brokers and insurance agents) or non-financial companies (such as marketers) with whom we have joint marketing agreements. We do not provide account numbers for marketing purposes.

- When Legally Required

We may disclose certain information about you to selected credit reporting agencies and when we are otherwise legally required to do so (such as in response to a subpoena), to prevent fraud, or to comply with a legally permitted inquiry by a government agency or regulator.

RESTRICTIONS ON DISCLOSURE OF NON-PUBLIC, PERSONAL HEALTH INFORMATION

National Penn does not disclose your non-public, personal health information to non-affiliated third parties (including government agencies) or our affiliated companies, except as authorized by you or to perform insurance functions (for example, obtaining an insurance policy or administering an insurance claim) as allowed by and in accordance with applicable law.

SHARING WITHIN THE NATIONAL PENN FAMILY

National Penn is made up of a number of companies, called affiliates, that work together to bring you the financial products/services you want and expect. We are permitted under law to share information about our experiences or transactions with your or your account (such as balance and your payment history with us) with companies related to us by common control or ownership ("affiliates.")

We are also permitted under law to disclose nonpublic personal information about you to "nonaffiliated third parties" (i.e., third parties that are not members of our corporate family) in certain circumstances. For example, we may disclose nonpublic personal information about you to such third parties to assist us in servicing your loan or account with us; to government entities in response to subpoenas; and to credit bureaus. We do not disclose any nonpublic personal information about you to any other third parties, except as permitted by law.

We may disclose all of the information we collect, as described above, to companies that perform marketing services on our behalf or to other financial institutions with which we have joint marketing agreements.

Otherwise, we do not share customer information with outside companies for purposes of selling their products and services to you. We do not sell "customer lists" to outside companies.

OPT-OUT CHOICES
You have two choices regarding affiliate credit sharing and affiliate marketing:

- Affiliate Credit Sharing Opt-Out:

The Fair Credit Reporting Act gives you the right to request us not to share certain credit information (such as specific information on your credit report), other than as permitted by law, with our affiliates.

- Affiliate Marketing Opt-Out:

Federal law gives you the right to limit some but not all marketing from our affiliates and requires us to give you this notice to tell you about your choices to limit Marketing from our affiliates. You may limit our affiliates in the National Penn family of companies, such as our insurance, securities, or trust affiliates, from marketing their products or services to you based on your personal information that we collect and share with them. This information is that which National Penn has on file such as details about your income or financial status, payment credit or account history.

You may opt out of one or both of the choices above. You may opt out at any time. If you previously opted out of one or both of the choices, you do not need to do so again, even if you have a closed account, as your choices will apply until you tell us to change your selection.

To out out, you may call us at 1.800.822.3321. You will need to provide your full name, address, social security number and telephone number and your opt-out selection choice. Note that opt-outs will take effect as soon as reasonably practicable, generally within a 30 day time period from the date your opt out is recorded.

JOINT ACCOUNTS
Each person may separately make privacy choices, and joint account holders may make privacy choices for each other. If only one joint account holder makes a privacy choice, that preference is applied to the entire account.

PROTECTING YOUR PRIVACY
We do not sell customer lists or individual customer information. We do not disclose any information about our customers, or former customers, to anyone, except as permitted by law. Any information we disclose comes from the sources described above and may include, among other things, your name, address and telephone number. We restrict access to your information to those employees who need to know that information in order to provide products/services to you, or to affiliates and other third parties for the purposes described previously. We require all companies with whom we share your information to keep it confidential and they may only use your information for the products/services requested or as permitted by law.

We have established a set of internal controls and procedures to maintain the confidentiality of your information in accordance with our policies, to maintain the accuracy of your information and to keep such information current and complete. We also provide you with various sources of

account information, including account statements, telephone banking, on-line banking, and electronic banking. If at any time you discover that any of your information is inaccurate, outdated, or incomplete, please call or write us at the telephone number or address listed on your account statement, bank records, or other documentation. We investigate customer inquiries or notifications regarding inaccurate information fully and promptly.

INVESTMENT AND TRUST RELATIONSHIPS

We recognize and acknowledge that all our clients have high expectations of privacy regarding account relationships they maintain with any of our companies within the National Penn Family. Accordingly, other than non-financial information recorded on our internal records to recognize you as our client, your nonpublic information is not shared with any third party unless it is required in the course of properly servicing your relationship or as required by law. Please contact your relationship manager if you have any questions regarding the privacy of your information.

RESTRICTIONS ON DISCLOSURE OF NON-PUBLIC PERSONAL HEALTH INFORMATION

We do not disclose your non-public personal health information to non-affiliated third parties (including government agencies) or our affiliated companies, except as authorized by you or to perform insurance functions. (For example, obtaining an insurance policy, or administering an insurance claim), as allowed by and in accordance with applicable law.

Thank you for choosing National Penn. If you have questions or would like more information, please call our customer service center at 1.800.822.3321.

Dated June 2009

Exhibit C

Mutual Shareholder Services, LLC's

Customer Information Privacy Policies and Procedures

General Information

Purpose and Scope

The purpose of this Compliance Manual is to act in accordance with Rule 38a-1. Rule 38a-1 requires fund boards to adopt written policies and procedures designed to prevent funds from violating federal securities laws. These policies are in accordance with but not limited to Title V of the Graham-Leach Bliley Act and the Bank Secrecy Act.

This document, along with the "Transfer Agent Policies and Procedures Manual", "General Compliance Manual" and the "Fund Accounting Policies and Procedures Manual", encompass the job functions that Mutual Shareholder Services, LLC ("MSS") performs for its clients.

Chief Compliance Officer and Responsibilities

The Chief Compliance Officer ("CCO") for Mutual Shareholder Services, LLC is Gregory B. Getts. The CCO is responsible for ensuring that MSS and its employees perform their responsibilities in a manner that meets the SEC's compliance regulations.

Compliance Coordination With the Funds

This Compliance Manual and related compliance information is supplied to the chief compliance officer of each fund that Mutual Shareholder Services, LLC services. MSS is not responsible for compliance coordination with any other service providers contracted by the fund.

Mutual Shareholder Services Privacy Policy

In the course of doing business with Mutual Shareholder Services, you share personal and financial information with us. We treat this information as confidential and recognize the importance of protecting access to it.

Information Systems

Mutual Shareholder Services, LLC uses internally designed and maintained accounting and transfer agent systems. Access to mutual fund computer records within these systems are limited to appropriate personnel through the use of passwords and access rules. Physical hardware other than desktop terminals is located in a separate area that is subject to restricted access rules.

Disclosure of Customer Information

We do not sell information about current or former customers to any third parties, and we do not disclose it to third parties unless necessary to process a transaction, service an account, or as otherwise permitted by law. We may share that information with companies that perform services for Mutual Shareholder Services. When we enter into such a relationship, our contracts restrict the companies' use of our customer information, prohibiting them from sharing or using it for any purposes other than those for which they were hired.

External Service Providers

Mutual Shareholder Services, LLC utilizes the following external organizations to provide specific services to MSS and the funds that its services. Each vendor's contract has been reviewed for the appropriateness of their privacy and confidentiality policies and procedures.

Organization	Services Provided
Thompson Financial	Pricing Service (Thompson One System)
RemitPro	Check new accounts against OFAC and SDN Lists
Keane Tracers,	Inc. Lost Shareholder Searches
Iron Mountain	Off-site Storage

Collection of Customer Information

You may provide information when communicating or transacting with us in writing, electronically, or by phone. For instance, information may come from applications, requests for forms or literature, and your transactions and account positions with us. On occasion, such information may come from consumer reporting agencies and those providing services to us.

Security of Customer Information

We maintain physical, electronic, and procedural safeguards to protect your personal information. Within Mutual Shareholder Services, access to such information is limited to those who need it to perform their jobs, such as servicing your accounts, resolving problems, or informing you of new products or services.