Birchcroft Investments, LLC
225 Walden St, 4A, Cambridge, MA 02140
BirchcroftInvestments.com • 617.249.3777

Matthew Raher, Fund Manager
mraher@birchcroftinvestments.com

Birchcroft Investments, LLC: Privacy Policy

Updated: October 1, 2023

Information Collected and Shared

The privacy policy statement is given to clients at the initial signing of the client contract and mailed or emailed with client consent once annually, or if the policy is updated. The CCO will document the date the privacy policy was delivered to each client for each year if an annual delivery is required. Birchcroft collects or may collect non-public personal information about clients from the following sources:

- Information it receives from them on applications or other forms;
- Information about their transactions with Birchcroft or others;
- Information it receives from consumer reporting agencies; and
- Information it receives from tax or other service professionals.

Below are the reasons for which Birchcroft may share a client's personal information:

- With specific third parties as requested by the client (see 'Sample of Authorization to Share Designated Information');
- For its everyday business purposes – such as with a broker-dealer to process client transactions and maintain client account(s); with a document storage provider to store books and records of Birchcroft; with an accountant or attorney to provide professional services to Birchcroft; or to respond to court orders, regulatory requests, and legal investigations.

Once a client's information is in the possession of a third party, Birchcroft no longer has control over its protection.

Birchcroft will notify the client if it changes how it shares a client's personal information, requesting prior approval when pertinent.

If a client decides to close his or her account(s) or becomes an inactive customer, Birchcroft will continue to adhere to the privacy policies and practices as described in this Policies and Procedures manual, as updated.

Birchcroft uses various methods to store and archive client files and other information. Third party services or contractors are chosen and used with an awareness of the importance Birchcroft places on both firm and client information security. Birchcroft also restricts access to clients' personal and account information to those employees who need to know that information to provide products or services to its clients. In addition to electronic protection, procedural safeguards, and personnel measures, Birchcroft has implemented reasonable physical and digital security measures at all office locations and to all remote work devices.

The names of Birchcroft's current and former access persons can be found at the end of this privacy policy.

In addition to Birchcroft's listed access persons, any IT persons or other technical consultants employed at the firm may also have access to non-public client information at any time. An on-site or off-site server that stores client information, third-party software that generates statements or performance reports, or third-party client portals designed to store client files all hold the potential for a breach of non-public client information.

The firm uses password protection on all computers and carefully evaluates any third-party providers, employees, and consultants with regard to their security protocols, privacy policies, and/or security and privacy training.

The cybersecurity system is tested at least annually and monitored on a continuous basis.

Guidelines for cyber security testing are laid out on the firm's Policies and Procedures manual and include the following activities, among others:

- Attempt to access Firm devices to ensure that proper passwords are in place to prevent access;
- Access systems with the proper password to ensure that two-factor authentication has been activated, where available;
- Attempt to restore a sample of files and records to ensure that the restoration process is sufficient and properly configured.

The results from the annual test will be documented and used as an opportunity to update the Cyber Security & Information Security Policy.

Identity Theft

The SEC and CFTC (U.S. Commodity Futures Trading Commission), and many state regulators, have published rules concerning identity theft encouraging or requiring investment advisers to train firm personnel to recognize "red flags" in this area. While many of these provisions are also covered in the firm's broader privacy and AML policies, the list below is a brief non-exhaustive listing of the items and information that all Birchcroft personnel should monitor to guard against any breach of a client's identity:

SAFEGUARDING IDENTIFYING INFORMATION

- Individual client's social security numbers
- Corporate or other entity client's tax identification numbers
- Individual driver's license number or other personal identification card
- Passport numbers
- Financial account numbers (credit card, bank, investment, etc.) and any accompanying passwords or access codes

POTENTIAL CAUSES OF IDENTITY INFORMATION BREACHES

- Loss or theft of computers and/or other equipment
- Hacking of computer networks
- Inadvertent exposure of client information to unauthorized individuals (non-locked files, files left on desk, cleaning services, shredding services, etc.)
- Physical break-ins / theft

Birchcroft personnel are instructed to notify and report to the firm's CCO, or other designated principal, if they detect or have reason to believe that any of the above shown red flag activities may have occurred or if any of the red flag information listed may have been stolen or leaked by any firm personnel. The CCO or principal is then tasked with investigating the report and taking appropriate actions. The non-exhaustive list of possible follow-up actions includes notification of the parties involved, notification of appropriate regulatory officials if required, taking remedial actions to assist in the recovery of the stolen information, and possible sanctions of firm personnel if deemed necessary.

Staff Training

On an annual basis, Birchcroft will conduct a firm-wide training session to ensure that staff members are properly trained and equipped to implement the above policies. New staff members will receive training, led by the CCO, within one (1) month of their initial hire date. An at-least annual review, update, and acceptance of this Policy by the CCO will suffice as the CCO's regular training.

Diminished Capacity & Elder Financial Abuse

As a fiduciary to clients, Birchcroft is required to report any suspected exploitation of vulnerable clients to the proper authorities under federal and state statutes. Elderly clients may be particularly vulnerable to financial abuse, as are clients of all ages that may be suffering from a diminished capacity (an impaired mental state or condition). If financial abuse is suspected, Birchcroft may find it necessary (or be required) to share certain account information with a limited partner's emergency contact, their family, and/or legal, government, and other regulatory authorities.

Records

Birchcroft will retain records for at least 5 years after the year in which the record was produced, or as otherwise required by law. With respect to disposal of non-public personal information, Birchcroft will take reasonable measures to protect against unauthorized access to or use of such information in connection with its disposal.

Birchcroft takes the privacy and confidentiality of all its clients and personnel very seriously. It will continue to make and document any changes needed to promote the security of non-public information.

List of Access Persons

"Access Person": Any of Birchcroft's supervised persons who have access to non-public information regarding any client's purchase or sale of securities, or information regarding the portfolio holdings of any reportable fund, or who is involved in making securities recommendations to clients, or who has access to such recommendations that are non-public.

- **Matthew T Raher,** Chief Compliance Officer

Opt-In Rights and Procedures

In order for Birchcroft to share any non-public personal information ("NPI") about an investor with a non-affiliated third party, that investor must provide Birchcroft with a signed statement in which the investor makes an affirmative, written declaration allowing the Firm to share that confidential information. Without this 'opt-in' authorization, Birchcroft is prohibited from sharing confidential information with non-affiliated parties.

Written 'opt-in' authorization may include e-mails, text messages, or forms similar to the 'Sample of Authorization to Share Designated Information' listed below. All authorizations will be kept on record according to the Firm's policies and procedures, as updated.

There is no 'opt-in' authorization required for any disclosure of investor NPI made by the Firm to service providers or joint marketers, and it is not required for the disclosure of confidential information in the following circumstances:

- For resolving consumer or customer disputes or inquiries;
- To persons holding a legal or beneficial interest relating to the investor;
- To persons acting in a fiduciary or representative capacity on behalf of the investor;
- To provide information to agencies assessing Birchcroft's compliance with industry standards;
- To provide information to the Firm's attorneys, accountants, and auditors;
- In connection with a proposed, or actual, sale or merger of the Firm;
- To respond to a regulator's examination of the Firm; or
- To comply with a civil, criminal, or regulatory investigation by federal, state, or local authorities.

Sample of Authorization to Share Designated Information

Client Name(s): _____

Client Account Number(s): _____

The above shown client(s) authorize Birchcroft to share designated information concerning the above shown account(s) with the party(ies) listed below. This shared information may include but not be limited to the following information:
(initial next to each applicable item to allow sharing)

1) _____ Registration of Account(s), Type of Account(s), and Ownership Information

2) _____ Custodian for Account(s) (or other information about where account assets are held)

3) _____ Holdings and Asset Allocations for Account(s)

4) _____ Suitability Information (Income, Net Worth, etc.)

5) _____ Investment Strategies For Account(s)

6) _____ Other: _____

Below is the name and contact information of the parties to which Birchcroft is authorized to release the information indicated above:

_____

_____

_____

_____

_____ _____

Client Signature / Date Client Signature / Date