



O'Keefe Stevens Advisory, Inc.
One Bausch & Lomb Place, Suite 920
Rochester, New York 14604
(585) 340-6538
www.okeefestevens.com

Privacy Policy

O'Keefe Stevens Advisory, Inc., a registered investment advisory and financial planning firm, is committed to safeguarding the confidential information of its clients. We hold all personal information provided to our firm in the strictest confidence.

The records we maintain include all personal information that we collect from you in connection with any of the services provided by O'Keefe Stevens Advisory. For purposes of this policy, **customer information** includes non-public personal information maintained by the Firm or on its behalf, including information maintained by third-party service providers.

We have never disclosed information to non-affiliated third parties, except as permitted by law, and do not anticipate doing so in the future. If we were to anticipate such a change in our Firm's policy, we would be prohibited under the law from doing so without advising you first.

As you know, we use health and financial information that you provide to us to help you meet your personal financial goals and have established the following procedures to mitigate any real or perceived infringements of your rights of privacy:

How We Protect Your Information

We limit access to your information by our associated persons to only:

1. those who have a business or professional reason for knowing;
2. non-affiliated parties as permitted or required by law (for example, to execute transactions or coordinate with your accountant or attorney); or
3. those required by judicial or regulatory process.

We maintain a secure office and computer environment designed to protect your information from unauthorized access or use, including administrative, technical, and physical safeguards.

The categories of non-public personal information that we collect depend upon the scope of your engagement and may include information about your personal finances, health (where relevant to planning), transactions, and information from consumer reporting agencies, if obtained.



Sharing Information with Third Parties

For unaffiliated third parties that require access to your personal information—such as custodians, financial service providers, consultants, auditors, and technology vendors—we require confidentiality and expect them to safeguard your information.

We may share your information as necessary to service your account, comply with legal or regulatory requirements, or as otherwise permitted by law.

We remain responsible for protecting your information, including information maintained by third-party service providers on our behalf.

Federal and state regulators may review Firm records as permitted by law.

We do not provide personally identifiable information to mailing list vendors or solicitors for any purpose.

Vendor Oversight and Due Diligence

We carefully evaluate third-party service providers that may have access to client information. As part of our vendor due diligence process, we consider the nature of the services provided and evaluate appropriate safeguards, which may include information security controls, confidentiality obligations, cybersecurity practices, and other measures designed to protect client information.

We periodically review vendors based on the sensitivity of the information they receive and expect them to maintain safeguards appropriate to the services they provide.

Technology & Cybersecurity

Recognizing the expanded use of Internet and technology-based systems, O'Keefe Stevens Advisory is committed to protecting your personal information from unauthorized access or use.

We utilize reasonable administrative, technical, and physical safeguards designed to:

- Protect against unauthorized access
- Detect and respond to potential security incidents
- Maintain the confidentiality and integrity of your information

While no system can be guaranteed to be completely secure, we continuously evaluate and enhance our safeguards.



Artificial Intelligence (AI) Tools

O'Keefe Stevens Advisory may utilize commercially available artificial intelligence ("AI") tools to assist employees with administrative tasks, drafting communications, research, data analysis, and other internal business functions.

The Firm does **not** input client non-public personal information ("NPI"), including personally identifiable financial information, account numbers, Social Security numbers, or other confidential client data into publicly accessible AI platforms.

Where AI tools are used, they are subject to the Firm's internal information security policies and employee training. The Firm utilizes business or enterprise versions of AI platforms, where available, that provide enhanced security, administrative controls, and contractual privacy protections appropriate for business use.

AI-generated content is reviewed by Firm personnel before being relied upon or communicated to clients. AI tools are used to support—not replace—the professional judgment of our advisors and staff.

Incident Response & Client Notification

If we become aware of unauthorized access to or use of sensitive customer information, we will take prompt action to investigate and contain the incident.

Where required by law, we will notify affected clients as soon as practicable, including providing information about the incident and steps that may be taken to protect against potential harm.

Data Retention & Disposal

Your information will be maintained for the duration of our relationship and for the period required by applicable laws and regulations.

After this period, we will securely dispose of such information in a manner designed to prevent unauthorized access or use.



Your Role in Protecting Your Information

You also play an important role in protecting your information:

- Do not share your login credentials, passwords, or PINs
- Notify us immediately if you suspect unauthorized activity

We may request certain identifying information (such as Social Security number or account details) to verify your identity when you contact us or when we contact you. However, we will never request your passwords or PINs.

If You Have Questions or Concerns

If at any time you believe your information has been compromised or have questions regarding this policy, please contact:

Carly Flanigan, Chief Compliance Officer
(585) 340-6538

Your concerns will be promptly investigated.