WHITE OAK
FINANCIAL MANAGEMENT INC
REGISTERED INVESTMENT ADVISOR

Customer Privacy Policy Notice

Effective Date: June 1, 2026

INTRODUCTION

This Privacy Notice describes how White Oak Financial Management, Inc. ("White Oak," "we," "us," or "our") collects, uses, shares, and protects your non-public personal information. This notice is provided to you at the time you enter an advisory relationship with us and annually thereafter as required by Regulation S-P and the privacy provisions of the Gramm-Leach-Bliley Act.

OUR COMMITMENT TO YOUR PRIVACY

White Oak is committed to maintaining the confidentiality, integrity, and security of the personal information that is entrusted to us. We do not sell your information to third parties. We do not share your information with third parties for their marketing purposes. We share your non-public personal information only as necessary to provide you with financial advisory services and as permitted or required by law.

INFORMATION WE COLLECT

Categories of Non-Public Personal Information We Collect:

We collect the following categories of non-public personal information about you in order to provide financial advisory services:

- Identification Information: Name, address, date of birth, social security number, driver's license number, and other government-issued identification numbers
- Financial Information: Assets, income, account balances, net worth, financial history, investment experience, investment objectives, and financial goals
- Account Information: Account numbers, transaction history, holdings, trading activity, and account balances
- Health Information: Information about your health to the extent it is needed for the financial planning and strategy development process
- Transaction Information: Information about transactions between you and third parties
- Professional and Personal Information: Employment status, occupation, business associations, marital status, dependents, and beneficiary information
- Other Information: As needed for planning purposes, you may choose to share credit reports, health information, outside investment holdings and personal information from your attorney, accountant, or insurance professional.

Sources of Information:

We gather this information from the following sources:

- Applications and Forms: Information you provide when opening an account, engaging our advisory services, or updating your profile
- Transactional Activity: Your account activity, including trading history, account balances, deposits, withdrawals, and investment holdings

- Communications: Information you provide during meetings, phone calls, emails, or other communications with us
- Other Sources with Your Consent: Confidential information you share and authorize us to obtain from third parties such as your insurance professional, attorney, accountant, or other financial institutions.

HOW WE USE YOUR INFORMATION

We use your non-public personal information to:

- Provide the investment advisory services described in our Form ADV Disclosure Brochure
- Develop and implement financial strategies and investment recommendations tailored to your needs
- Maintain and service your investment advisory accounts
- Process your transaction requests and instructions
- Monitor your accounts and provide performance reporting
- Communicate with you about your accounts and our services
- Respond to your inquiries and requests
- Comply with applicable laws, regulations, and regulatory requests
- Protect against fraud, unauthorized transactions, and other legal risks
- Maintain our books and records as required by law

We limit access to your information within our firm to only those individuals who need it to provide financial services to you or to comply with legal and regulatory requirements.

INFORMATION WE SHARE

We do not sell your non-public personal information to anyone.
We do not provide your personal information to mailing list vendors or solicitors.

Categories of Information We May Share:
We may share the categories of non-public personal information described above only as necessary to provide advisory services to you and as permitted by law.

Categories of Third Parties Who May Receive Your Information:
We may share your non-public personal information with the following categories of non-affiliated third parties as necessary to service your accounts and provide advisory services:

Financial Service Providers:

- Broker/dealers who execute securities transactions on your behalf
- Custodians who hold and safeguard your securities and cash (such as Fidelity Investments)
- Mutual fund companies and technology/service providers as required to serve clients' needs
- Insurance companies for insurance products you purchase
- Transfer agents and clearing firms

Professional Service Providers:

- Attorneys, accountants, and auditors who assist us in providing services to you or who provide services to our firm (when you have authorized such sharing or it is necessary to provide services you have requested)
- Compliance consultants and regulatory filing services

Operational and Technology Service Providers:

- Software vendors who provide portfolio management, performance reporting, and client relationship management systems
- Data processing and cybersecurity service providers
- Document management and storage providers
- Cloud computing and backup service providers

Other Parties:

- Federal and state securities regulators who may review our records and your personal information as permitted by law
- Other parties as required by law or legal process (such as court orders or subpoenas)

We do not have any affiliated companies and therefore do not share your information with affiliates.

Permitted Sharing Under Federal Law:
Federal law permits us to share your non-public personal information with these non-affiliated third parties without providing you with notice or an opportunity to opt out when the sharing is necessary to:

- Effect, administer, or enforce a transaction that you request or authorize
- Process or service a financial product or service that you request or authorize
- Maintain or service your account with us
- Comply with legal or regulatory requirements

These "servicing exceptions" allow us to share your information with broker/dealers to execute your trades, with custodians who hold your assets, with mutual fund companies to administer your investments, and with technology vendors who help us manage your accounts—all without requiring your specific permission each time or providing opt-out rights.

Confidentiality Requirements for Third Parties:
When we share information with non-affiliated third parties, we:

- Require them by written contract to protect the confidentiality of your information
- Permit them to use your information only for the specific purposes for which we disclose it
- Stress the confidential nature of the information being shared
- Conduct due diligence on their information security practices before engaging them
- Monitor their performance and security practices on an ongoing basis

YOUR PRIVACY RIGHTS AND CHOICES

Federal Opt-Out Right:

Federal law gives you the right to limit some but not all sharing of your non-public personal information. Specifically, federal law gives you the right to opt out of certain sharing of your information with non-affiliated third parties for purposes other than servicing your account.

Because we only share your information with non-affiliated third parties for the purposes of servicing your account and providing the advisory services you have requested (as described above), and we do not share your information with third parties for their own marketing purposes, there is currently no information sharing from which you need to opt out under federal law.

If our information sharing practices change in the future such that we begin sharing your information for purposes other than servicing your account, we will provide you with a revised Privacy Notice explaining your opt-out rights and how to exercise them before implementing such changes.

Special Requirements for California, Connecticut, Massachusetts, New Mexico, and Vermont Residents:
If you are a resident of California, Connecticut, Massachusetts, New Mexico, or Vermont, state law provides you with additional privacy protections beyond federal law.

Under these state laws, we will not share your non-public personal information with non-affiliated third parties for purposes not directly related to servicing your account unless you affirmatively provide your written consent ("opt-in") to such sharing.

To date, we have not engaged in any information sharing that would require your opt-in consent under these state laws, and we do not anticipate doing so in the future without first obtaining your express written authorization.

If you are a resident of one of these states and have questions about your enhanced privacy protections, please contact us using the information provided below.

HOW WE PROTECT YOUR INFORMATION

We maintain physical, electronic, and procedural safeguards that comply with federal standards to protect your non-public personal information from unauthorized access and use.

Our Comprehensive Information Security Program:

We have adopted a comprehensive Information Security Program designed to:

- Ensure the security and confidentiality of customer information
- Protect against any anticipated threats or hazards to the security of customer information
- Protect against unauthorized access to or use of customer information
- Protect against the risk of identity theft

Physical Security Measures:

- Secured office premises with controlled access to all entrances and exits
- Visitor restrictions—visitors are only allowed in office areas with confidential client information on an escorted basis
- Locked file storage—client files are physically locked during non-business hours
- Security systems and alarm monitoring during non-business hours

- Secure disposal of records—shredding is required when disposing of any paper records containing confidential client information
- Locked server rooms with limited access to key personnel

Electronic Security Measures:

- Strong password requirements with alphanumeric and special character combinations
- Required password changes after specified time periods
- Multi-factor authentication employed whenever possible
- Automatic device locking after failed login attempts
- Automatic device locking after periods of inactivity
- Encryption of client information stored on or transferred via portable devices (laptops, tablets, external hard drives, USB drives, smartphones)
- Firewall protection and anti-virus/anti-malware software
- Regular security patches and software updates
- Password-protected wireless network connections (WPA/WPA2 encryption)
- Secure destruction of hard drives before disposal of old computers and storage devices
- Passwords never provided via email or through web pages accessed via email links
- Electronic requests for client information or changes confirmed via written communication or phone verification

Administrative Security Measures:

- Background checks for all employees, including unlicensed staff
- Background check requirements for vendors with access to office premises (maintenance, janitorial services)
- Limited access to client information based on business need—supervised persons may access information only when necessary to service accounts or provide advisory services
- Written confidentiality policies and procedures
- Employee training on confidentiality and security procedures
- Annual security audits conducted by qualified professionals
- Annual review and testing of the Information Security Program
- Incident Response Program for detecting, responding to, and recovering from cybersecurity breaches
- Service provider oversight and due diligence
- Immediate termination of access for departing employees

Employee Requirements and Accountability:
Our employees and affiliated persons are required to:

- Protect the confidentiality of your information at all times
- Access your information only when necessary to service your account or provide advisory services
- Secure physical files when leaving their desks
- Lock client files during non-business hours
- Shred documents when disposing of physical files containing client information
- Never share electronic passwords or access credentials
- Set electronic devices to require re-login after periods of inactivity

- Use and regularly update firewalls, anti-virus, and anti-malware software
- Encrypt all client information on portable electronic devices
- Password-protect smartphones and set auto-lock functions
- Report any suspected unauthorized access to client information immediately

Employees who violate our Privacy Policy or Information Security Program are subject to disciplinary action, up to and including termination.

Incident Response Program:
We maintain a comprehensive Incident Response Program to:

- Detect cybersecurity incidents and unauthorized access to customer information promptly
- Assess the nature and scope of any incidents
- Contain and control unauthorized access
- Notify affected clients as required by law if sensitive information is compromised (within 30 days of incident)
- Take corrective action to prevent future incidents
- Document all aspects of incidents and our response
- Conduct post-incident reviews and implement improvements

Third-Party Service Provider Oversight:
We require all service providers who have access to your information to:

- Maintain appropriate physical, electronic, and administrative safeguards
- Protect the confidentiality of your information
- Use your information only for the purposes for which we engage them
- Contractually agree to confidentiality and security requirements
- Promptly report any cybersecurity incidents or breaches to us (within 72 hours)
- Provide notification to affected individuals on our behalf if required

We conduct due diligence reviews of our service providers' information security practices before engaging them and monitor their performance and security practices on an ongoing basis.

Visitor and Termination Procedures:

- All visitors to our office are restricted to one entry point for each building
- Visitors are not permitted in areas where client information is stored or accessible unless escorted by a supervised person
- Upon termination, employees must return all records containing client information
- Terminated employees' access to client information (both physical and electronic) is immediately blocked
- Terminated employees must surrender all keys, IDs, access codes, and badges
- Remote electronic access, voicemail, email, internet access, and passwords are immediately disabled for terminated employees

USE OF ARTIFICIAL INTELLIGENCE TECHNOLOGY

White Oak may utilize artificial intelligence (AI) and machine learning technologies to support certain operational and analytical functions, which may include (but are not limited to):

- Meeting Summaries (In person, phone call, or Zoom)
- Data analysis and reporting
- Research and information gathering
- Administrative task automation

All AI-assisted processes are subject to human review and oversight. Investment decisions and personalized advice are made by White Oak's investment professionals, not by AI systems. White Oak maintains appropriate controls and supervision over AI-assisted processes to ensure accuracy, compliance, and alignment with client interests.

Your personal and confidential information used in AI-assisted processes remains subject to White Oak's privacy and information security policies and receives the same protections as described in this Privacy Notice.

ELECTRONIC COMMUNICATIONS AND SOCIAL MEDIA

White Oak may communicate with clients through email, text messaging, video conferencing, and social media platforms. All electronic communications are subject to the same confidentiality and privacy protection as other communications.

However, clients should be aware that email and other electronic communications may not be completely secure and could potentially be intercepted by unauthorized parties. We employ encryption and other security measures where possible to protect electronic communications.

If you prefer not to receive certain types of electronic communications or wish to communicate exclusively through more secure channels, please contact us using the information provided below to make alternative arrangements.

White Oak maintains policies and procedures governing the use of social media and electronic communications to ensure compliance with securities regulations and protect client information.

RECORD RETENTION

Personally identifiable information about you will be maintained while you are a client of White Oak, and for the period thereafter that records are required to be maintained by federal and state securities laws (generally five years after the termination of the advisory relationship). After the required retention period, information may be securely destroyed.

CHANGES TO THIS PRIVACY NOTICE

We reserve the right to modify this Privacy Notice at any time to reflect changes in our privacy practices, legal requirements, or business operations. We will notify you in advance if we make material changes to how we collect, use, or share your non-public personal information.

If we make material changes, we will provide you with a revised Privacy Notice before implementing the changes. You will have the opportunity to opt out of any new information sharing practices that are materially different from those described in this Privacy Notice.

Annual Delivery:

We are required by law to deliver this Privacy Notice to you annually, in writing, for as long as you maintain an advisory relationship with us. You may request a copy of our current Privacy Notice at any time by contacting us using the information provided below.

HOW TO CONTACT US

If you have any questions about this Privacy Notice, wish to request a copy of this notice, want to exercise any privacy rights available to you, or have concerns about how we handle your information, please contact:

Brent A. Ford, Chief Compliance Officer
White Oak Financial Management, Inc.
1270 Hendersonville Road, Suite 4
Asheville, North Carolina 28803
Phone: (828) 274-7844
Email: info@wofm.us

You may contact us by telephone, email, regular mail, or in person during normal business hours.

REGULATORY INFORMATION

This Privacy Notice is provided pursuant to Regulation S-P (17 CFR Part 248), which implements the privacy provisions of the Gramm-Leach-Bliley Act. Additional information about White Oak Financial Management, Inc. is available on the SEC's website at www.adviserinfo.sec.gov.

Federal and state securities regulators may review our firm records and your personal records as permitted by law.

White Oak Financial Management, Inc.
June 1, 2026