April 2020

Privacy Policy & Information Security

The privacy policy statement is given to clients at the initial signing of the client contract and mailed or emailed once annually. The CCO will document the date the PPS was mailed to each client for each year. Lamorinda Financial Planning, LLC, (DBA East Bay Divorce Financial Planning) collects nonpublic personal information about you from the following sources:

- Information we receive from you on applications or other forms
- Information about your transactions with us or others
- Information we receive from a consumer reporting agency

We do not disclose any nonpublic personal information about you to anyone, except previously agreed or as required or permitted by law. If you decide to become an inactive customer, we will adhere to the privacy policies and practices as described in this notice.

East Bay Divorce Financial Planning restricts access to your personal and account information to those employees or contractors who need to know that information to provide products or services to you. We maintain physical, electronic, and procedural safeguards to guard your nonpublic personal information.

The following employees will manage nonpublic information: Elizabeth W. McClelland and David Smith.

The following individuals also have access to this nonpublic information: Elizabeth W. McClelland, and David Smith.

The following systems may be vulnerable to a breach of your nonpublic information: NordVPN, Avast Premium Security, Wealthbox.com, DropBox, Google Business Mail, Microsoft Office Suite, Perfect Audit, Family Law Software, Right Capital, Quickbooks, LastPass, Grammerly, Hello Sign, Zoom Video conferencing, Adobe Acrobat, and Sfax – secure fax.

To mitigate a possible breach of the private information Lamorinda will encrypt all data that individuals have access to or use password sensitive documents. The security system will be reviewed, tested, and monitored at least annually.

We have taken extensive measures to safeguard the privacy and integrity of the information that we gather, store, and archive during its normal business practices. Computer security measures have been instituted where applicable including passwords, virtual private network (VPN), premium antivirus and backup protection, and encryption. All employees are informed and instructed on various security measures including the non-discussion and/or sharing of client information, always removing client files from desktops or working areas that cannot be locked or secured, and proper storage of client securities files in locked files or other secured location. We use various methods to store and archive client files and other information. All third party services or contractors used have been made aware of the importance we place on both firm and client information security. In addition to electronic and personnel measures we have implemented reasonable physical security measures at our home and meeting office locations.

We will retain records for at least 5 years, or as otherwise required by applicable state or federal law. With respect to disposal of nonpublic personal information, we will take reasonable measures to protect against unauthorized access to or use of such information in connection with its disposal.