Privacy Policy and Practices

Of

Wesling Financial Planning Services Corp.

We value your trust. We are committed to the responsible:

a) Management;
b) Use; and
c) Protection;

of your **Personal Information**.

This notice describes how we collect, disclose, and protect your **Personal Information**.

We may obtain your **Personal Information** from:

a) You; and
b) Your agreements with us.

Based on the type of service **You** obtain from us, **Personal Information** such as:

a) Your name;
b) Your address;
c) Your income;
d) Your expenses;
e) Your investments;
f) Your insurance policies;
g) Your estate documents
h) Your taxes;
i) Your debts and payments;
j) Your assets; or
k) Your net worth;

may be gathered from applications, data gatherers, goal setting instruments, and discussions.

To serve **You** and service our business relationship with **You**, from time to time it may be necessary to share certain information with others. This will only be done with your **prior permission.**

Again, only with your prior permission, we may share certain non-identifying **Personal Information** with potential service and product providers to work toward achieving your life financial goals, such as:

a) Your age;
b) Your gender
c) Your marital status; and
d) Your smoker/non-smoker status;

This information may be used to help obtain information concerning products and services including, but not limited to insurance policies, tax preparation and estate documents.

We will not tell, sell or distribute any identifying **Personal Information** or **Personal Health Information** (medical records, information provided to us about illness, disability, or injury) without either **your prior written, verbal, or electronic approval** under any circumstances, unless required by court order.

We use manual and electronic security measures to maintain:

a) The confidentiality; and
b) The integrity of;

Personal Information either obtained by us or delivered to us. We use these procedures to guard against unauthorized access.

Some techniques we use to protect **Personal Information** include:

a) Secured files;
b) User authentication;
c) Encryption;
d) Firewall technology; and
e) Anti-spam and anti-spyware software technologies.

We are responsible for and must:

a) Identify information to be protected;
b) Provide an adequate level of protection for that information; and
c) Grant access to protected information only to those people who must use it in the performance of their job-related duties.

Employees who violate these policies will be subject to disciplinary actions, possibly resulting in employment termination.

At the start of our business relationship and on an annual basis, we will provide **You** a copy of our current Privacy Policy.

The current Privacy Policy remains in force for your **Personal Information** even when a business relationship either does not yet, or no longer exists between us.

If Something Bad Happens to You or a Loved One:

a) Contact your bank and all other companies with whom you have a financial relationship;
b) Contact any one of the three major credit bureaus to place a fraud alert on your credit report (this alerts all three credit bureaus):
    a. Equifax 800.525.6285
    b. Experian 888.397.3742
    c. Trans Union 800.680.7289

c) Report unauthorized charges or unauthorized new accounts to the credit issuer and credit bureaus (phone and writing are best);
d) Close accounts you feel have been compromised;
e) Request and review copies of your credit reports through www.annualcreditreport.com;
f) File a police report as soon as you can; and
g) Keep copies of any written correspondence to the credit bureaus and police.

Keep up with the latest in tips to avoid scams by visiting the Federal Trade Commission's website, www.ftc.gov/idtheft or phone the FTC at 1.877.ID.THEFT.