Acceptable Use Policy

Effective Date: 9/1/2024

Version: 1.0

1. Purpose

This policy outlines the acceptable use of all Family Law Software (the "Company") information systems, networks, and data, including but not limited to the Company's Cloud application, IT equipment, email, internet access, and data storage. The purpose of this policy is to protect the Company's assets, ensure data security, comply with legal obligations, and promote a secure and professional work environment.

2. Scope

This policy applies to all employees, contractors, consultants, temporary staff, and any other individuals who have access to the Company's information systems and data, regardless of location or device.

3. Acceptable Use

Users are granted access to Company resources to perform their job duties. Acceptable use includes, but is not limited to, the following:

- Using Company assets for legitimate business purposes.
- Protecting all account credentials (e.g., passwords, multi-factor authentication codes) and not sharing them with anyone.
- Handling confidential and proprietary information in accordance with the Company's data security and privacy policies.
- Promptly reporting any security incidents, vulnerabilities, or suspected policy violations to [e.g., the IT Security team or a designated manager].
- Complying with all applicable laws and regulations.

4. Prohibited Use

The following activities are strictly prohibited. This list is not exhaustive, and the Company reserves the right to determine what constitutes inappropriate use.

- Engaging in illegal or fraudulent activities.
- Accessing, creating, storing, or transmitting any content that is obscene, defamatory, harassing, or discriminatory.
- Installing or using unauthorized software on Company-owned devices or networks.
- Attempting to bypass or disable security measures, including but not limited to firewalls, antivirus software, and access controls.
- Unauthorized sharing of confidential, proprietary, or sensitive Company data.
- Introducing malicious code, viruses, or other harmful software into the Company's systems or network.
- Sending unsolicited mass emails ("spam").
- Using Company resources for personal gain or commercial activities unrelated to the Company's business.
- Violating any intellectual property rights of others, including copyright, patents, and trademarks.

5. Employee-Owned Devices (Bring Your Own Device - BYOD)

When an employee's personal device is used to access Company information systems, the employee agrees to comply with this policy and any related BYOD policy. The Company reserves the right to monitor, manage, and/or wipe data on any device connected to its network or used to access its systems to ensure compliance and security.

6. Monitoring and Enforcement

The Company reserves the right to monitor all user activity and content on its systems and networks to ensure compliance with this policy. Violations of this policy may result in disciplinary action, up to and including termination of employment, and may also be subject to legal action.

7. Policy Acknowledgement

All users must read and agree to this policy as a condition of using the Company's information systems.

---

8. Signatures

I have read and understand the [Your Company Name] Acceptable Use Policy and agree to abide by its terms.

Name: _____ Signature: _____
Date: _____