Artificial Intelligence (AI) Use and Governance Policy

As of: July 1, 2026

1. Purpose

This policy defines how Family Law Software governs the use of Artificial Intelligence (AI) in its software development processes and outlines the framework for future AI capabilities within its Family Law SaaS platform. It is intended to ensure security, confidentiality, compliance, and responsible AI usage, particularly in the context of handling sensitive legal and financial information.

2. Scope

This policy applies to:

- All employees, contractors, and third-party vendors
- AI tools used during software development, testing, and operations
- Planned and future AI features within the SaaS product
- All customer data processed, stored, or accessed by AI systems

3. Current Use of AI

At present, Family Law Software:

- **Does not deploy AI within its production software platform**
- **Does not use AI to process customer data in live environments**

AI tools may be used internally for:

- Code generation and review
- Development productivity enhancements
- Documentation drafting and summarization
- Testing support

Controls for Development AI Usage:

- No confidential customer data, personally identifiable information (PII), or sensitive legal data may be entered into external AI tools
- Only approved AI tools vetted by security and legal teams may be used

- Developers must adhere to secure coding and data handling standards when using AI-assisted outputs
- All AI-generated code is subject to human review and standard QA/security processes

4. Data Protection and Privacy

Family Law Software maintains strict controls to ensure:

- Customer data is **never used to train third-party AI models**
- Data is processed in accordance with applicable laws and regulations (e.g., GDPR, CCPA, and relevant financial data regulations)
- Encryption is enforced:
    - Data in transit (TLS 1.2 or higher)
    - Data at rest (AES-256 or equivalent)
- Access to data is role-based and audited
- Data minimization principles are applied

5. Future AI Capabilities (Planned)

Family Law Software intends to introduce AI-driven features to support legal case analysis. These may include:

- Case outcome insights
- Document analysis and summarization
- Pattern recognition across case data
- Decision-support tools for legal professionals

Pre-Deployment Requirements:

Before any AI functionality is released:

- Formal **security risk assessments** will be conducted
- Models will undergo **bias, fairness, and accuracy evaluation**
- Customers will be clearly informed of AI usage and capabilities
- Opt-in/opt-out mechanisms will be provided

6. AI Governance Framework

Family Law Software follows these principles:

a. Human Oversight

- AI outputs will not replace professional legal judgment
- Users retain full control over decisions and actions

b. Transparency

- AI-generated outputs will be clearly labeled
- Documentation will explain how AI features function at a high level

c. Accountability

- Internal ownership assigned for AI systems (Product, Engineering, Security)
- Incident response procedures include AI-related risks

d. Fairness and Bias Mitigation

- Models will be evaluated for unintended bias
- Continuous monitoring and improvement processes will be implemented

7. Third-Party AI Vendors

When using third-party AI providers:

- Vendors must meet Family Law Software's security and compliance standards
- Data Processing Agreements (DPAs) must be in place
- Vendors must not retain or use customer data for training without explicit authorization
- Regular vendor risk assessments will be conducted

8. Security Controls

- AI-related systems will follow the same security standards as core infrastructure
- Logging and monitoring will include AI interactions where applicable
- Secure SDLC practices apply to all AI-integrated features
- Regular penetration testing and vulnerability assessments will be conducted

9. Compliance

This policy aligns with:

- Applicable data protection regulations (e.g., GDPR, CCPA)
- Industry-standard security frameworks (e.g., SOC 2, ISO 27001 principles where applicable)
- Financial-sector expectations for data handling and risk management

10. Incident Management

Any suspected AI-related security or privacy incident will:

- Be reported immediately to the Security Team
- Follow established incident response procedures
- Include customer notification where required by law or contract

11. Policy Review and Updates

This policy will be:

- Reviewed at least annually
- Updated as AI capabilities evolve
- Approved by executive leadership and security stakeholders