

Ai Safety in Law

A Quick Guide for Legal Teams Using AI Tools Responsibly

Why It Matters

AI tools like ChatGPT and Zapier can dramatically improve efficiency — drafting documents, summarizing content, and automating admin tasks. But **in a legal environment, data privacy, client confidentiality, and professional ethics come first**. Misuse of AI could risk client trust, bar compliance, or even privilege protection

AI Use That's Generally OK

These use cases are typically safe if no confidential or identifying information is included:

- Drafting or refining boilerplate content (e.g., general engagement letters, standard contract clauses)
- Summarizing public case law, articles, or statutes
- Rewriting internal communications or training materials
- Generating outlines for marketing content or blog posts
- Automating non-sensitive workflows (e.g., intake confirmations, task reminders)
- Creating first drafts of non-client-facing content (e.g., SOPs, email templates)

Tip: If it's general, public, or non-client-specific — it's likely AI-safe.

AI Use That's Not OK in Legal Practice

These actions risk ethical breaches, client exposure, or compliance issues — and should be avoided unless you're using secure, approved AI tools:

- Uploading or referencing client names, case details, or documents
- Drafting legal briefs or motions using AI without review
- Inputting contracts, discovery material, or evidence into AI tools
- Automating client communications without oversight
- Using AI to conduct legal research without verification
- Sharing anything that would fall under attorney–client privilege

Reminder: Tools like ChatGPT, Zapier, and Pipedrive are not built for privileged or confidential data. Most do not offer encryption, access controls, or jurisdictional protections lawyers require.

