Law Society of Ireland

ARTIFICIAL INTELLIGENCE (AI) USE POLICY

Law Society of Ireland, Blackhall Place, Dublin 7

Tel: +353 1 881 5768 | Email: solicitorservices@lawsociety.ie | www.lawsociety.ie

TEMPLATE

Artificial Intelligence (AI)
Use Policy

[Law firm name]

Prepared for use by law firms in Ireland

[Date]

Document Title	Artificial Intelligence (AI) Use Policy
Version	***[1.0]***
Date Adopted	***[DD/MM/YYYY]***
Approved By	***[Name / Role / Board]***
Policy Owner	***[Name / Role]***
Next Review Date	***[DD/MM/YYYY]***
Classification	***[Internal / Confidential]***

ARTIFICIAL INTELLIGENCE (AI) USE POLICY

How to use this template

GUIDANCE NOTE: These pink sections are for law firms to adapt the template for their own firm. They should be deleted from the final version of your AI Use Policy. Please read this section in full before filling in the template.

This template has been developed for small and medium-sized law firms in Ireland that wish to adopt a proportionate, practical AI policy. It takes account of the EU AI Act (Regulation (EU) 2024/1689), the General Data Protection Regulation (GDPR), and Irish data protection law and practice.

You do not need to be a technology specialist to complete this template. The guidance notes (displayed in pink boxes like the one above) explain each section in clear, plain language and tell you what to consider when completing this AI Use Policy. All guidance boxes should be removed from the final version of this AI Use Policy document.

Key Steps to Completing This AI Use Policy

KEY PRINCIPLES

1. **Read through the full template first** to understand its scope and structure before making any changes.
2. **Complete the placeholders** (displayed in red text in square brackets) using your firm's specific details.
3. **Tailor the Acceptable Use** section to reflect the AI tools your law firm currently uses or plans to use.
4. **Delete all guidance boxes** (pink-bordered boxes) before finalising this AI Use Policy document.
5. **Have this AI Use Policy reviewed** by an appropriate person within your law firm (e.g. a partner or director) and formally adopted.
6. **Circulate the final AI Use Policy to all Staff,** ensure it is incorporated into your firm's onboarding materials and provide training on it.

REGULATORY CONTEXT FOR IRISH LAW FIRMS

Two key pieces of EU legislation are relevant to AI use by Irish law firms:

- **The EU AI Act (Regulation (EU) 2024/1689)** is the world's first comprehensive AI law. It classifies AI systems into four risk categories (unacceptable, high, limited, and minimal risk) and imposes different obligations to each category. Most law firms are likely to use AI tools that fall into the "minimal risk" or "limited risk" categories, but each AI system must be assessed to confirm its category. The Act began applying in phases from February 2025.

- **The General Data Protection Regulation (GDPR)** applies whenever AI tools process personal data. This includes any use of personal data to train, test, or operate AI systems, as well as cases where the output generated by an AI system contains personal data. In Ireland, compliance is supervised by the Data Protection Commission (DPC).

This AI Use Policy template is designed to support law firms even if your law firm's current use of AI only is a limited (e.g. grammar-checking tools, search tools, or using AI for research). The structure provides a scalable framework that can grow alongside your law firm's adoptions and use of AI technologies.

1. Purpose and scope

GUIDANCE NOTE: This section explains the purpose of this AI Use Policy and identifies who it applies to. Your law firm should not need to change the substance significantly but do fill in your firm name and consider whether to extend the scope to contractors, temporary staff, or interns.

1.1 Purpose

The purpose of this AI Use Policy is to establish clear rules and practical guidance for the responsible use of artificial intelligence (AI) tools and systems within the law firm. It aims to ensure that AI is used in a manner that is lawful, ethical, transparent, and consistent with the law firm's obligations under applicable law, including:

- The EU Artificial Intelligence Act (Regulation (EU) 2024/1689)
- The General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR")
- The Data Protection Act 2018 (as amended)
- Any sector-specific regulations relevant to the law firm's activities

1.2 Scope

This AI Use Policy applies to all partners, directors, employees, **and [insert additional categories (if any) such as contractors, temporary staff or interns]** ("Staff") of **[insert law firm name]** ("the law firm"). It covers all use of AI tools, whether provided by the law firm or accessed independently by Staff, and whether used on law firm-issued devices or personal devices for work-related purposes.

2. Key definitions

GUIDANCE NOTE: These definitions in this section are based on terminology used in the EU AI Act and the GDPR. You may add law firm-specific terms if necessary, but you should avoid changing any of the legal definitions provided.

- **Artificial Intelligence (AI):** A machine-based system designed to operate with varying levels of autonomy, that may exhibit adaptiveness and that infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. (Art. 3(1) EU AI Act)
- **AI System:** Any software or service that uses AI techniques, including but not limited to large language models (e.g. ChatGPT, Microsoft Copilot, Google Gemini), image generators, automated decision-making tools, and analytics platforms.
- **Personal Data:** Any information relating to an identified or identifiable natural person. (Art. 4(1) GDPR)
- **Special Category Data:** Personal data revealing racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic or biometric data, health data, or data concerning sex life or sexual orientation. (Art. 9 GDPR)
- **Deployer:** A natural or legal person that uses an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity. Under the EU AI Act, most law firms using third-party AI tools will fall within the definition of a "deployer."
- **Data Protection Impact Assessment (DPIA):** A formal process for assessing the impact of data processing operations on the protection of personal data, required under Art. 35 GDPR where processing is likely to result in a high risk to individuals.
- **Human Oversight:** The requirement that a natural person reviews, validates, or has the ability to override AI-generated outputs before they are acted upon.

3. Governance and oversight

GUIDANCE NOTE: Even in a small law firm, responsibility for AI governance must be clearly assigned. This role may be held by a partner, the office manager, or the person responsible for compliance. If your law firm already has a Data Protection Officer (DPO) or designated data protection lead, they may be a natural fit for this responsibility. In very small law firms, it is acceptable for a single person to hold multiple roles.

3.1 AI lead

[Insert Role/Title] is designated as the law firm's AI lead. The AI lead is responsible for:

- Maintaining an up-to-date register of all AI tools used within the law firm (see Appendix A).
- Reviewing and approving the use of new AI tools before they are deployed.
- Ensuring compliance with this AI Use Policy and with all applicable legal and regulatory requirements.
- Acting as the first point of contact for Staff queries related to AI use.
- Coordinating with the law firm's Data Protection Officer or data protection lead on matters involving personal data.
- Reporting to management on AI-related risks and incidents.

3.2 AI register

The law firm shall maintain an up-to-date register of all AI tools and systems in use (see Appendix A). For each tool, the register shall record, at a minimum:

- The name and provider of the tool,
- The purpose for which the tool is used,
- The types of data it processes,
- The AI Act risk classification, and
- The date on which it was approved for use

GUIDANCE NOTE: A template AI register is included in Appendix A. You should complete this register with the AI tools your law firm currently uses. Common examples for law firms include Microsoft Copilot, ChatGPT, Grammarly, Canva's AI features, Google Gemini, accounting software with embedded AI functionality, and CRM tools that offer AI-assisted analytics.

4. Acceptable use of AI

GUIDANCE NOTE: This section sets out rules governing day-to-day Staff use of AI tools. You should tailor the lists below to reflect the specific activities and AI tools used within your law firm. The three-tier structure (permitted, permitted with approval, prohibited) provides Staff with clear, simple guidance. Add or remove items as appropriate to ensure this AI Use Policy accurately reflects your law firm's operations and risk profile.

4.1 General principles

All use of AI within the law firm must be guided by the following principles:

- **Lawfulness:** AI must only be used in compliance with applicable Irish and EU law.
- **Transparency:** Staff must be open about when and how they use AI. Clients, customers, and other stakeholders must be informed where AI has materially contributed to a deliverable or decision.
- **Human oversight:** AI generated outputs must always be reviewed by a competent person before they are relied upon, shared externally, or used to make decisions that may affect individuals.
- **Accuracy:** Staff must verify the accuracy of AI-generated content. AI systems can produce outputs that appear credible but are incorrect ("hallucinations").
- **Data minimisation:** Only the minimum amount of data necessary should be entered into any AI tool. Personal data and confidential information must not be entered into external AI tools unless expressly approved.
- **Accountability:** Individuals who use an AI tool remain fully responsible for the outputs generated. AI must not be treated as a substitute for professional judgement.

4.2 Categories of use

The table below sets out the law firm's classification of AI use cases. Staff must review this section before using AI for a new task. If a proposed use is not listed, Staff should consult the AI lead before proceeding.

PERMITTED USES (NO APPROVAL REQUIRED)

- Grammar and spell-checking of documents
- Summarising publicly available information for internal research
- Generating first drafts of internal communications or marketing copy
- Using AI scheduling or calendar management tools
- Translation of non-confidential materials

4.2 Categories of use

PERMITTED WITH APPROVAL

- Using AI to assist in drafting client-facing documents (subject to mandatory human review)
- Analysing anonymised or pseudonymised datasets
- Deploying AI tools that interact with clients (e.g. chatbots)
- Using AI-generated images or content in external publications
- Integrating new AI tools or plugins into law firm systems

PROHIBITED USES

- Entering personal data, confidential client information, or trade secrets into public AI tools
- Using AI to make final decisions on recruitment, dismissal, or disciplinary matters affecting individuals without human review

GUIDANCE NOTE: Review the items above carefully to ensure they reflect your law firm's risk appetite and nature of legal work. You may wish to move certain items between the "permitted", "Permitted with approval" and "prohibited" categories. For example, a conveyancing practice may wish to permit AI-assisted title review and due diligence under the "permitted with approval" category, whereas a criminal defence law firm may prohibit any AI use that involves client case details being entered into external tools. A litigation team might permit AI-assisted legal research and case law summarisation but require senior solicitor sign-off before any AI-drafted pleading is filed. See Appendix A for illustrative use cases across common practice areas.

4.3 Use of public AI tools

Public AI tools are those accessible over the internet without a dedicated enterprise agreement (e.g. the free versions of ChatGPT, Google Gemini, or similar services). The following additional rules apply to the use of public AI tools:

- No personal data, special category data, or confidential business information may be entered into a public AI tool.
- Staff must assume that any data entered into a public AI tool may be stored, used for training, or disclosed by the provider.
- Public AI tools must not be used for any task involving client-confidential or commercially sensitive material.

Where the law firm has an enterprise licence for an AI tool (e.g. Microsoft 365 Copilot with data protection commitments), different rules may apply. The AI lead will maintain a list of approved enterprise tools and communicate the applicable requirements to Staff.

5. Data protection and GDPR compliance

GUIDANCE NOTE: Your law firm will also be subject to data protection obligations. Accordingly, any AI-related processing activities should be added to your law firm's Data Protection Policy/Privacy Notice and related records such as the record of processing activities (ROPA). The screening checklist below helps you decide when a data protection impact assessment (DPIA) is needed. If in doubt, consult the Data Protection Commission's website for published guidance.

5.1 Core requirements

When any AI tool processes personal data, the law firm must ensure the following:

- **Lawful basis:** A valid lawful basis under Article 6 GDPR has been identified. Where special category data is processed, a condition under Article 9 must also be satisfied.
- **Transparency:** Data Subjects must be informed about the law firm's use of AI in its Privacy Notice. This includes the purposes of processing, the categories of personal data involved, and whether any automated decision-making is taking place.
- **Data minimisation:** Only data that is adequate, relevant, and limited to what is necessary may be processed through AI tools.
- **Storage limitation:** Data that is entered into AI tools must not be retained longer than necessary. Where possible, prompts and outputs should be deleted once the task is complete.
- **Purpose limitation:** Data that is entered into AI tools must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- **Accuracy:** Data that is entered into AI tools should be accurate and, where necessary, kept up to date. In deploying any AI system, it is important to check the accuracy of outputs not only initially but also over the entire time the system is in use.
- **Security:** Appropriate technical and organisational measures must be in place, including access controls, encryption, and vendor security assessment to ensure the AI tools integrity and security posture.
- **International transfers:** Where AI providers process data outside the EEA, appropriate safeguards, such as Standard Contractual Clauses (SCCs) or an adequacy decision must be in place before any processing occurs.

5.2 Data protection screening checklist

Before deploying a new AI tool that processes personal data, complete the following screening questions.

Question	Yes/No	If Yes, Action Required
Does the AI tool process personal data?		Identify the lawful basis under GDPR Art. 6 (and Art. 9 if special category data is involved).
Is personal data transferred outside the EEA?		Ensure appropriate safeguards are in place in accordance with GDPR Chapter V (e.g. SCCs or an adequacy decision).
Does the AI tool involve automated decision-making affecting individuals?		Comply with Art. 22 GDPR, including providing meaningful information about the logic involved and ensuring the right to human review.
Is the AI tool profiling individuals?		Conduct a Data Protection Impact Assessment (DPIA) under Art. 35 GDPR.
Could the AI tool create a high risk to individuals' rights and freedoms?		A DPIA is mandatory. If residual risk remains high after mitigation, consult the Data Protection Commission (DPC) (Art. 36 GDPR).
Does the AI tool use publicly scraped data that may include personal data?		Assess whether the processing is compatible with original purpose of collection (Art. 5(1)(b) GDPR)

GUIDANCE NOTE: If you answer "Yes" to any question, discuss the matter with your data protection lead or DPO. A full DPIA may be required. The Irish Data Protection Commission publishes a list of processing operations that require a DPIA under Irish law, which may be consulted when making this assessment.

5.3 Automated decision-making

Under Article 22 of the GDPR, individuals have the right not to be subject to decisions based solely on automated processing (including profiling) that produce legal or similarly significant effects. Where the law firm uses AI in any decision-making process that affects individuals (e.g. clients, Staff, or job applicants), it must ensure that:

- A human being reviews and approves the decision before it is communicated or implemented.
- The individual is informed that AI was used in the decision-making process.
- The individual is afforded their rights, including the right to obtain human intervention, to express their point of view, and contest the decision.

6. EU AI Act compliance

GUIDANCE NOTE: Most law firms using standard, off-the-shelf AI tools (e.g. ChatGPT, Microsoft Copilot, Grammarly) will fall within the category of "deployers" of "minimal risk" or "limited risk" AI systems. This means your obligations are relatively light, however, it is still essential to understand the risk categories and confirm the classification of any AI tools your law firm uses. If your law firm develops its own AI tools or uses AI in areas that may be considered high-risk under the EU AI Act (e.g. recruitment screening or decision-making tools that could significantly affect the individual's rights), your compliance obligations are significantly greater and you should seek specialist legal advice.

6.1 Risk classification

The EU AI Act classifies AI systems into four risk categories. All AI tools used by the law firm must be assessed against these categories and recorded in the AI Register (Appendix A).

AI Act Risk Category	Description including examples	Your Obligation
Unacceptable Risk (Prohibited)	Social scoring, real-time biometric identification in public spaces, manipulation of vulnerable groups	Must not be used under any circumstances
High Risk	AI used in recruitment, credit scoring, education, critical infrastructure, law enforcement	Must comply with strict requirements: risk management, data governance, technical documentation, transparency, human oversight, registration in EU database, cyber security
Limited Risk	Chatbots, emotion recognition, deepfake generators	Transparency obligations: users must be told they are interacting with AI Accountability: include information on which AI functions are enabled, human oversight. AI Literacy: ensure that staff that deals with the AI tool has sufficient knowledge of its operation and use.
Minimal / No Risk	Spam filters, AI-assisted drafting, scheduling tools, grammar checkers	No specific obligations, but best practice measures (e.g. human oversight, responsible use) should be followed.

6.2 Deployer obligations

As a deployer of AI systems, the law firm has the following obligations under the AI Act:

- **Transparency:** Where transparency is required (e.g. when using chatbots or emotion recognition tools), the law firm must ensure that individuals are clearly informed they are interacting with an AI system.
- **Monitoring**: The law firm must monitor the operation of high-risk AI systems it uses and must report serious incidents to the relevant authorities.
- **Record-keeping:** The law firm must maintain logs of AI system use as required by the provider's instructions.
- **Human oversight:** The law firm must ensure that staff responsible for overseeing high-risk AI systems have the appropriate competence, training, and authority to intervene, override, or suspend system outputs when necessary.
- **AI Literacy**: Under Article 4 of the AI Act, deployers must ensure that their staff and other individuals acting on their behalf who interact with AI systems possess a sufficient level of AI literacy. This requirement applies to all deployers, regardless of risk category of the AI system being used.

GUIDANCE NOTE: The AI literacy obligation under Article 4 of the EU AI Act applies from 2 February 2025. This requirement does not mean that staff must become technical experts. It requires that staff have a basic understanding of what the law firm's AI tools do, their limitations, and how to use them responsibly and safely. This AI Use Policy, combined with a short training session, will substantially assist your law firm in meeting this obligation.

7. Transparency and disclosure

7.1 Internal transparency

Staff must disclose the use of AI tools in their work in the following circumstances:

- When AI has materially contributed to a document, analysis, or recommendation that will be shared with colleagues for decision-making purposes.
- When AI has been used to draft client-facing communications.
- When recording the methodology of any work product where AI was used as a research or drafting tool.

7.2 External transparency

The law firm will inform clients and other external parties about its use of AI where:

- AI has been used in the preparation of a deliverable or advice (a brief disclosure is sufficient, e.g. "AI tools were used to assist in the preparation of this document. All content has been reviewed and approved by [Name/Role].")
- Customers or clients are interacting with an AI system (e.g. a chatbot on the law firm's website).
- Required by law, regulation or contractual obligation.

GUIDANCE NOTE: The level of disclosure should be proportionate. For routine tasks (e.g. grammar checking), no disclosure is needed. For substantive work products, a short footnote or cover note is good practice. Solicitors should have regard to the Law Society of Ireland's Generative AI Guidance on the use of AI in legal practice. The Law Society's Technology Committee has published professional guidance notes addressing the ethical and practical implications of AI for solicitors, including duties of competence, confidentiality, and supervision. The Law Society also maintains a Legal Tech Hub with dedicated AI resources. The Law Society Gazette regularly publishes articles on AI in legal practice. Barristers should refer to any guidance issued by the Bar of Ireland and the Legal Services Regulatory Authority (LSRA). The LSRA's regulatory framework and any technology-related guidance should also be monitored for updates.

8. Intellectual property

Staff must be aware of the following principles regarding intellectual property and AI-generated content that:

- The copyright status of AI-generated content is evolving and remains uncertain in many jurisdictions. Content generated solely by AI system may not qualify for copyright protection.
- Entering the law firm's proprietary materials, trade secrets, or unpublished work into external AI tools may compromise confidentiality or, depending on the provider's terms of service, may grant the provider a licence to use, store or further process that content. Such disclosures are prohibited unless expressly approved.
- AI-generated outputs may inadvertently replicate copyrighted material contained within the tool's training data or retrieved through its generation process. Staff must therefore review all AI-generated content for originality and ensure it does not infringe third-party rights before publishing or distributing it.
- The law firm's standard position is that any AI-generated work product created by staff in the course of their employment is owned by the law firm, subject to the law firm's existing employment contracts and intellectual property policies.

9. Training and AI literacy

GUIDANCE NOTE: Article 4 of the AI Act requires all deployers to ensure that staff have a sufficient level of AI literacy. For a law firm, this can be achieved through short internal briefings, online training modules, or a lunch-and-learn workshops. Ensure you keep records of who has completed training and when, as you may need to demonstrate compliance during audits or regulatory inquiries.

The law firm is committed to ensuring all staff have a sufficient level of AI literacy, as required by Article 4 of the EU AI Act. To this end:

- All staff will receive introductory training on this AI Use Policy and on the responsible use of AI within 30 days of the policy's adoption or within 30 days of joining the law firm, whichever is later.
- Refresher training will be delivered at least annually, or more frequently if the law firm adopts significant new AI tools, if material changes occur in legislation or regulation, or if emerging risks are identified through oversight activities.
- The AI lead will maintain accurate and up-to-date records of all training completed by staff.

Training will cover, at a minimum:

- A basic explanation of what AI is and how it works
- The law firm's Acceptable Use rules
- Relevant data protection considerations
- How to verify and critically assess AI-generated outputs
- How to report concerns, incidents or suspected misuse of AI tools

10. Third-party AI providers and procurement

Before the law firm engages any new AI tool or provider, the AI lead must assess the following:

- Whether the provider's terms of service permit the law firm's intended use of the AI tool, including any restrictions on professional, commercial or legal sector applicants.
- Where the provider processes and stores data, including the identity and location of any sub-processors and whether international transfers are involved.
- Whether the provider offers an enterprise version with enhanced privacy controls (e.g. contractual assurances that customer data is not used for training models).
- Whether a Data Processing Agreement (DPA) is required under GDPR Article 28 and, if so, whether the law firm is satisfied with the provider's data processing terms.
- The provider's security posture including certifications (e.g. ISO 27001, SOC 2), penetration testing practices, incident response processes and security track record.
- The provider's approach to AI safety, including bias mitigation, fairness testing, content moderation practices and mechanisms for handling harmful or inappropriate outputs.
- Whether the provider offers clear exit arrangements, including data export options, deletion commitments and portability of any law firm-generated data or work products should the law firm transition to a different provider in the future.

11. Incident reporting and breach management

Staff must report any AI-related incident to the AI lead without delay. Reportable incidents include:

- Accidental disclosure of personal data or confidential information through an AI tool.
- Discovery of biased, discriminatory, or materially inaccurate AI outputs, particularly where they have been relied upon in decision making or external work products.
- A security breach involving an AI system or third-party AI provider.
- Any use of AI that may breach this AI Use Policy or applicable law.

Upon receiving an incident report, the AI lead will assess and determine whether:

- The incident constitutes a personal data breach requiring notification to the Data Protection Commission within 72 hours under Art. 33 GDPR.
- The affected individuals must be notified under Art. 34 GDPR.
- A serious incident report must be submitted to the national AI supervisory authority under the EU AI Act.

12. AI Use policy review

This AI Use Policy will be reviewed at least [insert cadence e.g. annually], or more frequently if required by changes in law, technology, or the law firm's use of AI. The AI lead is responsible for initiating and coordinating each review.

Each review should consider:

- Whether the AI Register is complete and up to date
- Whether the Acceptable Use categories remain appropriate
- Whether any new legal, regulatory or professional requirements have come into force
- Whether any incidents, near-misses or operational issues indicate gaps or areas for improvement in this AI Use Policy.

13. Compliance and enforcement

All staff are required to comply with this AI Use Policy. Breach of this AI Use Policy may result in disciplinary action, up to and including dismissal, in accordance with the law firm's disciplinary procedures.

Where a breach of this AI Use Policy also constitutes a breach of GDPR, the EU AI Act, or any other applicable law, both the law firm and/or the individual concerned may be subject to regulatory investigation and sanction.

AI Use Policy approval

Approved By	***[Name, Title]***
Signature:	
Date:	***[DD/MM/YYYY]***
Effective from:	***[DD/MM/YYYY]***

Appendix A: AI register

GUIDANCE NOTE: Complete this register with every AI tool your law firm uses or plans to use. Review it each time the AI Use Policy is reviewed. Sample entries are included to illustrate how to fill it in. Delete or amend the sample entries as needed.

AI Tool	Provider	Purpose	Data Types	Risk Level	Approved	Review Due
Microsoft Copilot (365)	Microsoft	Drafting, summarising, email assistance	Internal docs, emails	Minimal	DD/MM/YY	DD/MM/YY
ChatGPT (Enter-prise)	OpenAI	Research, brainstorming, first drafts	Non-personal, non-confidential	Minimal	DD/MM/YY	DD/MM/YY
Grammarly Business	Grammarly	Grammar and tone checking	Document text	Minimal	DD/MM/YY	DD/MM/YY
Bloomberg Law	Bloomberg	Litigation analytics, brief analysis, points of law	Case data, legal research queries	Limited	DD/MM/YY	DD/MM/YY
Luminance	Luminance Technolo-gies	Contract review, due diligence, M&A document	Client docu-ments, contracts	Limited	DD/MM/YY	DD/MM/YY
Harvey	Harvey AI	Legal research, drafting, document analysis	Legal queries, case materials	Limited	DD/MM/YY	DD/MM/YY
Legora	Legora	Legal research, case law	Legal queries, case data	Limited	DD/MM/YY	DD/MM/YY
Robin AI	Robin AI	Contract drafting, review, and negotiation	Contracts, legal documents	Limited	DD/MM/YY	DD/MM/YY
DocuSign (AI features)	DocuSign	Contract lifecycle management, AI-assisted review	Contracts, signatory data	Minimal	DD/MM/YY	DD/MM/YY
[Tool Name]	[Vendor]	[Functionality]	[Data Input]	[Scope]	DD/MM/YY	DD/MM/YY

Appendix B: Staff Quick Reference Card

GUIDANCE NOTE: Consider printing this page and displaying it in a common area or circulating it as a one-page summary alongside the full AI Use Policy. It can also be used as a handout during training sessions.

Before Using Any AI Tool, Ask Yourself:

1. **Is the tool on our approved list? If not, check with the AI lead first.**
2. **Am I about to enter personal data or confidential information? If so, STOP – use an approved enterprise tool or anonymise the data.**
3. **Will I review the output before sharing or relying on it? You must always check AI outputs for accuracy.**
4. **Do I need to tell anyone that AI was used? If the output goes to a client or is used for a decision, disclose it.**
5. **Am I unsure about anything? Ask the AI lead – it is always better to check.**

Key Contacts

Role	Name	Contact
AI lead	*[Name]*	*[Email / Phone]*
Data protection lead / DPO	*[Name]*	*[Email / Phone]*
IT support	*[Name / Team]*	*[Email / Phone]*

Appendix C: Version History

Version	Date	Author	Changes
1.0	*[DD/MM/YYYY]*	*[Name]*	**Initial adoption**

This resource was developed by Pembroke Privacy in consultation with the Law Society of Ireland.

Solicitor Services Department
Law Society of Ireland,
Blackhall Place, Dublin 7,
D07 VY24