PRAXIS CONSULTING

AI Compliance First Pack

Version 1.0 - January 2026

Prepared by Praxis Consulting

This pack provides Irish solicitors' firms with practical, audit ready templates for managing AI use, vendor oversight and incident response under the new regulatory landscape.

Contents

AI compliance is now a live regulatory and professional risk that can land on a firm suddenly through everyday behaviour.

The EU AI Act (Regulation (EU) 2024/1689) has made AI a governance issue and firms need to know what AI systems are being used, for what purposes and what controls sit around that use.

The immediate danger for most firms is the unapproved AI already in the building. Risks that come from staff using personal accounts and unknown settings to summarise emails, rewrite letters, extract timelines or check" points and sometimes pasting client material in. This shadow AI use mostly leaves no reliable record of what input was, what was generated or what was verified. When that goes wrong, the consequences are usually felt through GDPR and the Data Protection Act 2018. Uncontrolled disclosure to third parties, unclear international transfers, weak security and the hard operational reality of breach readiness, including the requirement, where feasible, to notify the supervisory authority within 72 hours of becoming aware of a notifiable personal data breach.

Cyber expectations are tightening too through NIS2 (Directive (EU) 2022/2555) and the broader shift towards documented incident preparedness and supply chain discipline across the services and providers firms rely on.

On 11 November 2025, the Law Society of Ireland issued guidance on the ethical and responsible use of generative AI, anchoring it to core duties like confidentiality, competence, supervision and verification.

This pack is designed as the evidence layer that closes the gap quickly. Clear internal rules, a matter level risk gate, a verification record, vendor due diligence discipline and a same day incident playbook. The aim is that if you are asked what controls you have, you can answer with documents rather than assurances.

Implementation in 60 Minutes

This pack is designed for immediate use. In one hour, a partner or practice manager can adopt the AI Use Policy firm wide, integrate the AI Matter Risk Checklist into file opening procedures, store the Verification File Note in each matter template, circulate the Incident Response one pager and assign ownership of the Vendor Register to your Data Protection lead. These templates do not replace professional judgment but demonstrate it in action creating real, reviewable evidence of competence, compliance and client care.

1) Internal AI Use Policy (v1.0)

Document control

- Title: Internal AI Use Policy
- Version: 1.0
- Owner: Managing Partner / Risk Partner / Data Protection Lead
- Approved: _____
- Effective date: ___ / ___ / 2026
- Review date: ___ / ___ / 2026

1. Purpose

This policy sets rules for the safe and professional use of AI tools within the firm. It is intended to protect client confidentiality, ensure accuracy, support compliance (including data protection obligations) and produce clear evidence of oversight and verification on file.

2. Scope

Applies to all staff and consultants including partners, solicitors, trainees, paralegals, support staff and contractors.

3. Definitions

- AI tool: Any system that generates, summarises, classifies, drafts or analyses text, images, audio or data using automated models.
- Client data: Any information relating to a client or matter, including documents, messages, IDs, financial details or case strategy.
- Sensitive data: Special category data, criminal data, health data, children's data or any information that could materially harm a client if disclosed.

4. Core principles

1. Confidentiality first: Do not expose client data to tools or suppliers that are not approved.
2. Human responsibility remains: AI outputs are not authority. The fee earner remains responsible for the advice/work product.
3. Minimum necessary: Use the least amount of information required. Prefer anonymisation and abstraction.
4. Verification is mandatory: Any AI derived content used in a matter must be checked and recorded.

5. Transparency where appropriate: Where client communication or terms require it, disclose AI assisted workflows in a controlled way.
6. No automation of judgment: AI must not make final decisions on legal strategy, filings or client advice without human review.

5. Permitted uses (examples)

AI may be used for low risk support tasks only after applying the AI Matter Risk Checklist:

- summarising *non confidential* or anonymised text
- drafting neutral correspondence structures (not advice)
- reformatting, proofreading and plain English rewriting
- checklists, chronologies, action plans based on facts provided
- initial issue spotting prompts, provided outputs are treated as prompts and not conclusions

6. Prohibited uses

AI must not be used to:

- upload or paste unredacted client documents into unapproved tools
- generate final legal advice without full verification and partner oversight
- draft pleadings, affidavits, witness statements or settlement terms without explicit matter level approval and verification and then only using approved tools/workflows
- handle sensitive categories (children, criminal, medical, domestic violence, asylum/immigration status) unless the firm has a documented high scrutiny workflow and partner sign off
- create or alter evidence, transcripts or factual records
- make representations to a court without human verification and independent source checking

7. Approved tools and access

Approved AI tools list (maintained by the firm):

- Tool name: _____ Purpose: _____ Approved by: _____ Review date: _____
- Tool name: _____ Purpose: _____ Approved by: _____ Review date: _____

Rules:

- Use firm-managed accounts where possible.
- Personal accounts are not permitted for client related AI use.
- Do not enable optional settings that train models on firm/client content unless the firm has explicitly approved it and documented the risks.

8. Matter level process (required)

Before using AI on a matter:

1. Complete the AI Matter Risk Checklist
2. Apply anonymisation/redaction where feasible
3. Use only approved tools
4. After use, complete an AI Output Verification File Note if the output influences work product, correspondence, filings or client communication

9. Data protection and security controls

- Classify the information: public, internal, client confidential, sensitive
- Prefer abstracted prompts over raw documents
- Never input authentication details, bank details, medical details, criminal history or identifiers unless explicitly approved under a documented workflow
- Store AI outputs and file notes within the firm's matter management system where possible

10. Training and literacy

All staff must receive basic AI literacy training and updates on:

- permitted v. prohibited use
- confidentiality risks
- verification standards
- incident reporting routes

11. Monitoring and review

- The firm will review tool usage, incident logs and vendor assurances at least quarterly.
- This policy is reviewed at least every six months or on material regulatory/technology change.

12. Breaches of this policy

Any suspected breach must be reported immediately under the Incident Response One Pager. Failure to comply may lead to disciplinary action.

2) AI Matter Risk Checklist

AI Matter Risk Checklist v1.0
Matter: _____ File no: _____
Fee earner: _____ Supervisor/Partner: _____
Date: ___ / ___ / 2026

A. Intended AI use

☐ Summarise documents

☐ Draft structure (not final advice)

☐ Proofread / plain English rewrite

☐ Extract chronology / issues list

☐ Research support (note: primary sources still required)

☐ Other: _____

B. Data to be used

☐ Public / non confidential

☐ Internal firm info (non-client)

☐ Client confidential (redacted/anonymised)

☐ Client confidential (unredacted)

☐ Sensitive data (special category / criminal / children / medical)

C. Risk flags (tick any that apply)

☐ Urgent deadlines / limitation risk

☐ High value claim or major exposure

☐ Novel / complex point of law

☐ Vulnerable client or capacity concerns

☐ Children involved

☐ Criminal allegations / regulatory investigation

☐ Immigration/asylum status issues

☐ Domestic violence / protective orders

☐ Significant reputational risk

☐ Court filing or sworn evidence involved

☐ Third-party confidential material (bank, employer, insurer, medical)

D. Tool and controls

Tool to be used: _____
Account type: ☐ Firm-managed ☐ Personal (not permitted)
Inputs will be: ☐ Abstracted ☐ Redacted ☐ Unredacted (requires partner sign off)

E. Outcome and required controls (choose one)

Green (low risk):

☐ Approved to proceed with anonymised/redacted inputs

Required: file note if output used in work product

Amber (medium risk):

☐ Proceed only with partner awareness and enhanced verification

Required: AI Output Verification File Note + independent source checks + no unredacted uploads

Red (high risk):

☐ Do not use AI on this matter without partner sign off and a documented workflow

Default: avoid AI use for substantive content.

Decision: ☐ Green ☐ Amber ☐ Red
Partner sign-off (if Amber/Red): _____ Date: ___ / ___ / 2026

3) AI Output Verification File Note template

AI Output Verification File Note v1.0
Matter: _____ File no: _____
Fee earner: _____ Date/time: ___ / ___ / 2026 :

1. What AI tool was used

Tool name: _____
Access method: ☐ Firm account ☐ API via approved platform ☐ Other: _____
Purpose of use: _____

2. What information was provided to the tool

Information type: ☐ Abstracted summary ☐ Redacted text ☐ Unredacted (explain and confirm approval)
Was any client confidential data included: ☐ No ☐ Yes
If yes, describe at high level only: _____
Sensitive categories involved: ☐ No ☐ Yes (details): _____

3. Output used

Describe what the tool produced and what portion was relied on:

4. Verification steps completed (tick)

☐ Checked output against source documents on file

☐ Checked statutory references against official sources

☐ Checked case law references

☐ Removed any invented facts or assumptions

☐ Ensured tone and content meet professional standards

☐ Confirmed it aligns with client instructions and scope

☐ Confirmed it does not introduce limitation/deadline errors

☐ Supervisor review completed (if required)

5. Sources used to verify (list)

6. Decision

☐ Output used with amendments

☐ Output used as drafting scaffold only (substantially rewritten)

☐ Output not used (reason): _____

Fee earner signature: _____
Supervisor/Partner (if required): _____

---

4) Technology Supplier Due Diligence Checklist (v1.0)

Supplier Due Diligence Checklist v1.0
Supplier: _____ Product/service: _____
Reviewer: _____ Date: ___ / ___ / 2026
Purpose of procurement: _____

A. Basic information

- Supplier legal entity name: _____
- Primary contact: _____
- Support contact and hours: _____
- Contract term and renewal: _____

B. What data will be processed

Tick all that apply:

☐ Client identification data

☐ Financial data

☐ Legal advice/work product

☐ Court documents/pleadings

☐ Special category / criminal data

☐ Communications (email, portal messages)

☐ Metadata (usage logs)

Data locations (known): _____

C. Hosting and access

- Hosting model: ☐ Cloud ☐ On prem ☐ Hybrid
- Regions available: ☐ EU/EEA ☐ UK ☐ US ☐ Other: _____
- Admin access controls: ☐ MFA ☐ RBAC ☐ SSO ☐ Audit logs
- Staff access to customer data: ☐ No ☐ Yes (explain): _____

D. Security assurances

- Encryption in transit: ☐ Yes ☐ No ☐ Unknown
- Encryption at rest: ☐ Yes ☐ No ☐ Unknown
- Independent security certifications: ☐ ISO 27001 ☐ SOC 2 ☐ Other: _____
- Penetration testing evidence: ☐ Provided ☐ Not provided
- Data segregation (multi-tenant controls): ☐ Yes ☐ No ☐ Unknown

E. Sub-processors and onward transfers

- Sub-processors list provided: ☐ Yes ☐ No
- International transfers involved: ☐ No ☐ Yes (mechanism): _____
- Right to be notified of sub-processor changes: ☐ Yes ☐ No

F. GDPR and contract basics

- DPA available and reviewed: ☐ Yes ☐ No
- Controller/processor roles clear: ☐ Yes ☐ No
- Breach notification timeframe stated: ☐ Yes ☐ No
- Assistance with data subject rights: ☐ Yes ☐ No
- Data deletion/return on exit: ☐ Yes ☐ No
- Audit rights or equivalent assurances: ☐ Yes ☐ No

G. AI specific (if relevant)

- Does the product include AI features: ☐ Yes ☐ No
  If yes:
- Training on customer data: ☐ No ☐ Opt-in only ☐ Default on (not acceptable)
- Ability to disable training/retention: ☐ Yes ☐ No
- Explainability or logs of AI actions: ☐ Yes ☐ No
- Human override controls: ☐ Yes ☐ No

H. Operational resilience

- SLA uptime: _____
- Backup and recovery: ☐ Stated ☐ Unclear
- Incident response process described: ☐ Yes ☐ No
- Exit plan workable (data export formats, timeframes): ☐ Yes ☐ No

I. Decision

Risk rating: ☐ Low ☐ Medium ☐ High
Conditions before approval: _____
Approved: ☐ Yes ☐ No
Signed off by: _____ Date: ___ / ___ / 2026

5) Incident Response One Pager (v1.0)

Incident Response One-Pager v1.0
Covers: suspected data breach, cyber incident, accidental disclosure, AI misuse, vendor compromise.

1. What counts as an incident (examples)

- Client data sent to wrong recipient
- Lost device or compromised account
- Suspicious login or ransomware alert
- AI tool used with unapproved data or tool settings
- Vendor breach notification received
- Court filing or client letter contains incorrect AI generated content that could harm a client

2. Immediate actions (first hour)

- Contain: disconnect device, reset passwords, revoke access tokens, pause syncs
- Preserve evidence: screenshots, logs, emails, timestamps, affected files
- Stop the spread: notify internal lead, do not forward externally
- Record: start an Incident Log entry immediately

3. Internal notification

Incident lead: _____ (phone) _____
IT/security: _____
Data protection lead: _____
Managing partner: _____
Insurer contact: _____
External IT provider: _____

4. Minimum incident log fields

- Date/time discovered
- Who discovered it
- What happened (facts only)
- Data types involved
- Number of records/clients potentially affected
- Systems involved
- Containment steps taken
- Next actions and owner

5. Decision points (same day)

- Is this a personal data breach risk: ☐ Yes ☐ No ☐ Unknown
- Is there risk to client rights/freedoms: ☐ Yes ☐ No ☐ Unknown
- Is a vendor involved: ☐ Yes ☐ No
- Are court deadlines impacted: ☐ Yes ☐ No

6. External notifications

Any external notification should be coordinated by the firm's designated lead with appropriate professional judgment and advice where necessary:

- data protection regulator notifications (if applicable)
- affected client notifications
- insurers and third parties
- law enforcement where appropriate

7. Post incident actions

- root cause review
- document policy/process changes
- staff reminder or training
- vendor remediation or contract review

6) Vendor Risk Register (paste into Excel)

Copy these column headings into Excel:

- Supplier name
- Product/service
- Category (case management, email, portal, accounting, AI, storage, e-sign)
- Data types processed
- Hosting region
- Sub-processors confirmed (Y/N)
- International transfers (Y/N)
- Security assurance (ISO/SOC/none)
- MFA/SSO available (Y/N)
- Breach notification term (hours/days)
- Data export available (Y/N)
- Data deletion on exit (Y/N)
- Risk rating (Low/Med/High)
- Key controls/mitigations
- Contract renewal date
- Next review date
- Owner