AI Acceptable Usage Policy

General Comments -

* This is a template/precedent document only. It should be tailored as appropriate to suit the needs of each individual firm. All present and intended future use of AI must be audited and assessed by the firm prior to implementing an AI Acceptable usage policy.
* All sections should be considered and implemented as deemed appropriate for the firm. This cover page should not be included.
* The LQSI cannot accept any responsibility for any errors or omissions contained in this template document.
* The document should be reviewed regularly especially as AI is a complex and rapidly evolving area and guidance/codes of practice are still awaited from European institutions/ supervisory bodies.

Specific Comments –

* Article 3 of The EU AI Act defines an AI system as “a machine based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that for explicit or implicit objectives infers from the input it received how to generate outputs such as predictions, content, recommendations or decisions that can influence physical or virtual environments”.
* If the firm wishes to use AI systems, it must comply with the EU Artificial Intelligence Act and GDPR. A firm may decide not to use AI and that being the case should clearly communicate to staff a policy prohibiting the use of AI in the firm.
* Generally, the EU AI Act provides for the safe technical development and use of AI systems by providers (natural or legal persons who develop or has developed an AI system or a general purpose AI model) and deployers (natural or legal persons who use AI systems under their authority in a professional capacity – it does not apply to personal non-professional activity).
* The EU AI Act prohibits certain AI systems e.g. purposefully manipulative/deceptive AI systems which it categorises as constituting an unacceptable risk to human safety/rights. It permits other types of AI systems which it categorises as having a minimal, limited or high risk.
* The obligations for providers and deployers under the Act vary in accordance with the categorisation of the risk and it follows that there are greater obligations for high-risk AI systems or if the firm is a provider of an AI system as opposed to a deployer/user. In most cases, it is likely that the firm will be considered a deployer.
* High risk AI systems are listed in Annex I and Annex III of the EU AI Act and include AI systems used as safety components in products or AI systems used in areas such as employment/recruitment/credit scoring/determining access to education/law enforcement.
* For high-risk AI systems, guidance from the Commission is expected in 2026, However, under the EU AI Act users must take appropriate measures to:
  + ensure the system is used in accordance with the provider’s instructions
  + notify the provider/national supervisory body if there is an issue with system
  + ensure human oversight
  + keep system logs for at least 6 months
  + inform individuals if decisions are being made by AI about them
  + ensure data is representative and relevant
* Limited risk AI systems are systems which are not categorised as high risk but which create content or autonomously perform tasks and interact with individuals e.g. chatbots.
* Minimal risk AI systems pose insignificant/non-existent threat or potential for harm e.g. spam filters or ad blockers. These systems do not have additional obligations under the AI Act but would be subject to existing legislation.
* Transparency requirements apply to high risk, limited risk or general purpose AI so that natural persons know they are interacting with AI or that outputs from AI systems are identified as artificially generated or manipulated.
* The first step to drafting an AI Acceptable Usage Policy is for the firm to identify, understand and map the current use and/ or intended use of AI systems in the firm. Secondly, it must, audit and risk assess the AI systems - the firm should consider areas such as the AI system’s functionality, the suitability of data used to train the AI system, the reputation of the AI system developer and data protection features. Thirdly, it must decide what actions need to be taken to comply with the EU AI Act based on what the risk categorisation of the AI system is and whether it is a provider or deployer of an AI system. In most cases, it is likely that the firm will be considered a deployer.
* From 2 February 2025, Article 4 of the EU AI Act requires legal firms to ensure that staff using any AI system are AI literate and have a sufficient understanding of AI. This not only requires staff training but as referred to above, the firm must audit AI systems currently in use and assess potential future use of AI in the firm. For more guidance on this, firms should consult the Law Society Technology Committee Practice Direction dated 10 December 2024, “Navigating the EU AI Act: Ensuring AI Literacy in Legal Practices”.
* As personal data will be present at some stage of the lifespan of an AI system, GDPR works alongside the EU AI Act to protect persons in the processing of their data and both the EU AI Act and GDPR have some overlapping principles e.g. to prevent bias and discrimination. Article 22 GDPR is also relevant to the AI systems used for automated decision making. Firms therefore may have obligations under one or both Acts e.g. if a firm purchases an AI system such as a chatbot to talk to clients about their case, it will be a deployer under the AI Act and a processor under GDPR. It must therefore carefully map where its obligations lie and what parties are affected, and tailor an AI Acceptable Usage policy accordingly.
* National Bodies will be responsible for the overseeing and enforcing the EU AI Act in member states. The European AI Board, comprising of representatives from member states will coordinate implementation across the EU.
* The AI Office established within the Commission will be a centre for expertise in the development of AI and implement the act, especially in the area of general-purpose AI.
* Penalties under the EU AI Act will apply from August 2025 except for penalties for general purpose AI models which come into effect from August 2026.

The Legal Quality Standard of Ireland

March 2025

AI Acceptable Usage Policy

This document sets out the Firm’s policy for AI usage. It seeks to provide advice and assistance to you in your use of AI at work and also lists the rules about AI that you must follow.

These rules have been designed to ensure that the firm and you get the most from AI without imposing an unnecessary cost burden on the Firm. The Firm regards any breach of this policy as a serious matter. Any failure or refusal to comply with this policy is a disciplinary offence which may lead to disciplinary action, up to and including, dismissal without notice. You need to be aware that breach of the policy can lead to criminal and civil liabilities for the Firm.

I acknowledge receipt of XXXX, Solicitors’ AI Acceptable Usage policy and I agree to be bound by the rules contained in that document.

User Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Block Capitals)

Department: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(Block Capitals)

Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Managers Authorisation:

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(Block Capitals)

Position: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

AI Acceptable Usage Policy

Introduction

This policy applies to all solicitors and employees of [firm name] Solicitors.

Artificial intelligence (AI) is a powerful tool for performing specific tasks, problem solving and for generating new content. Whilst AI can be beneficial for performing certain tasks within the firm, AI suffers from significant and widespread security and integrity risks. Its accuracy is dependent on the data it trains/learns from and therefore has the potential to be used in ways that are inappropriate to the goals of the firm.

There are several risks associated with AI including:

1. Inaccurate or incomplete outputs: Generative AI can provide inaccurate or incomplete outputs or results based on misinformation or disinformation e.g. in 2023, a New York based firm was sanctioned by a US judge for including fictitious case citations generated by ChatGPT in a legal brief for a personal injury case. The intentional or accidental misuse of AI can cause reputational damage and loss for a firm and for the client.
2. Data Protection: Data processed by AI systems (including software, tools or a platform that uses AI technologies) may not be in accordance with data protection laws /GDPR and pose a threat to the privacy and confidentiality of client/firm data.
3. Inequality, discrimination and unfairness: AI can perpetuate inequality and discrimination if it has been trained in a way which results in data/algorithmic bias.
4. Cybersecurity – AI systems may be targeted by hackers/cyber criminals.

The above risks are taken into account in formulating the following AI Acceptable usage policy and the policy is designed to help you understand the firm’s expectations for the use of AI. As we integrate AI to improve efficiency and our professional service, this policy will be reviewed and updated.

Rules of Acceptable Usage

1. All AI Must be Authorised.

The use of an AI system must be authorised in advance by the Managing Partner- this includes software, apps or platforms that use AI to generate outputs. No AI systems are to be used by any fee earner/employee of the firm without the firm’s knowledge and authorisation.

If a fee earner/employee wishes to use an AI system reasoning that it is potentially beneficial to the firm, they must firstly provide a detailed proposal to the Managing Partner setting how the AI system will benefit the firm, for what purposes they intend to use it in their role along with any risks or difficulties they anticipate and any actions that are needed to mitigate or eliminate such risks or difficulties.

If following an assessment by the firm, the Managing Partner is satisfied that the AI system complies with legal /regulatory requirements, professional and ethical standards and is in the general best interests of the firm, the firm may authorise the use of AI to be used for a specific purpose for a specific role.

Only AI systems authorised by the Managing Partner may be used in the firm and only for purposes specified by the Managing Partner. In addition, only fee earners or employees who are specifically authorised to use AI systems and trained in this area may use them. Otherwise, the use of AI systems is not permitted by any fee earner or employee.

1. Fee Earner /Employee Training

All fee earners and employees using AI must have knowledge, skills and understanding about AI and must be trained in its use. No AI system may be deployed/used by any fee earner/employee until training has been completed to the satisfaction of the Managing Partner to ensure that fee earners and employees understand to the best extent (taking into account their technical knowledge, experience, understanding, training, the context the AI systems are to be used in and considering the persons on whom AI systems are to be used), the legal, technical, ethical and compliance requirements under GDPR/Data Protection Act and the EU AI Act. Users must be able to interpret AI outputs and recognise potential risks and harm that can be caused e.g. bias and errors in AI generated outputs.

Given the rapid development of AI, regular training and regulatory updates will be provided to staff. The firm will maintain records of staff training.

1. Transparency, Professional and Ethical Standards

AI is a tool to complement legal practice but it is not a substitute for human expertise. All AI content/results must be rigorously overseen and checked to ensure it is accurate, correct, up to date and tailored to the client’s needs. Clients rely on us for professional expertise, judgement, and our ability to interpret and critically analyse, which cannot be achieved by AI alone.

We have a fiduciary duty to our client and to always act honestly and in their best interests. It is also important that the client is fully informed and able to fully understand that we use AI tools to assist in providing the legal service with the involvement and oversight of the fee earner throughout the matter who always ensures that the legal services we provide meets the clients’ needs and best interests.

If AI is used by us to provide legal services to our clients, transparency should be prioritised, and AI usage must be disclosed to the client [ this may require amendment of the firm’s letter of engagement/terms and conditions/privacy statement]. This ensures that the client can consent to their data being processed by third parties and that the client can express any concerns that they may have and allow us to address them e.g. a client may require only human involvement for a sensitive matter or if a third party AI service is being used the client may have concerns about data security risks and have preferences about how their data is processed.

*It is important that if the firm wishes to use AI in other areas of the firm such as administration or HR that this is also referred to in the policy and that the firm is transparent about its usage and employees are aware of their interaction with AI. The firm must ensure that AI systems are free from bias and do not result in discrimination or unfairness which is a risk particularly in HR e.g. the screening of CVs or performance evaluation.*

*If AI is used for HR functions to make automated decisions, then this must be disclosed to the employees and data must be processed in accordance with GDPR / the Data Protection Act. The firm will also have to comply with the EU AI Act and to ensure that an employee’s health and safety and fundamental rights are protected from risks posed by AI. More official detailed guidance for employers from supervisory bodies/ EU institutions is expected in coming months. In the meantime, firms must be aware that AI used in areas such recruitment or performance assessment is high risk and deployers of AI in high-risk areas have significant obligations.*

1. The General Computer Usage Policy

The use of AI is subject to the firm’s general computer usage policy and in particular employees are reminded that:

* the installing and/or downloading of computer software (AI related or otherwise) onto the Firm computers is the exclusive responsibility of XXXX, Solicitors IT staff/External IT Providers
* firm computers may not be used for illegal purposes.
* the firm reserves the right to inspect all files/records stored on its network, servers, PCs, laptops, tablets etc.

1. Password Policy

The use of AI is subject to the firm’s password policy and employees using AI systems must apply password best practices.

1. Data Protection

Our Data Protection policy applies to the use of AI. Personal data used for AI systems must be processed in accordance with data protection policy and the EU AI Act.

The firm must also inform the client that their data will be processed by AI systems. If third party AI tools are used, the firm as part of its risk assessment must firstly verify in advance that there are adequate measures in place to protect data and ensure client confidentiality in accordance with Data Protection Act / GDPR e.g. in GPT models if personal details of the client or the firm are entered such as account/PPS numbers data may be stored or processed in ways that could be accessed by third parties beyond the firm’s control.

The processing of a client’s data on AI systems must be limited to the intended purpose and exclude excessive or irrelevant data.

The firm must ensure that AI systems/tools are securely integrated into its IT systems and are updated and monitored to ensure there are no vulnerabilities. Any data breach/near miss or suspicions regarding unauthorised access concerning AI systems should be reported in accordance with the firm’s policy and procedure for data breach handling and notification.

In accordance with the firm’s data protection policy and the EU AI Act, the firm will maintain records of data processing activities on AI systems/tools. The firm will also maintain records of AI systems design purpose and decision-making processes.

1. Audits, Accountability & Reporting Concerns

The firm will ensure that AI used within in the firm is monitored and audits will be conducted regularly to assess the performance of AI system and to ensure that same are operating fairly and in compliance with the EU AI Act.

The firm’s fee earners and employees must take responsibility for the use of AI systems/tools and should request assistance from the managing partner if they are unsure about any aspect of using AI. Any concerns or issues regarding the usage of AI should be reported as soon as possible to the Managing Partner so that appropriate actions can be taken.

Related Policies

General Computer, Internet, Intranet Email Usage Policy

Password Policy

Data Protection Policy

Data Breach Handling and Notification Policy and Procedure.

Policy on Keeping Staff updated on Regulatory Changes

Signed:

Dated:

Date of next review: