74Software

Version 1.0
Issued: July 2025

74Software Artificial Intelligence Policy

74Software
Artificial Intelligence Policy

74Software.com

Copyright © 74Software 2025. All Rights Reserved.

Summary

1. Objective

This policy sets out the standards adopted by 74Software in connection with Artificial Intelligence ("AI") technologies, aligning with the company strategy to support and promote emerging technologies while adhering to legal and regulatory requirements and 74Software client requirements.

The policy is designed to work alongside supporting AI Governance Framework and other 74Software policies while recognizing that developing a culture of responsible use of AI by all Colleagues is the responsibility of all involved within the organization.

2. Scope and Definition

This policy applies to all 74Software employees, contractors, consultants, temporary workers, and other agents worldwide (collectively referred to as "**Colleagues**").

AI is defined in the EU AI Act 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 receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments"

3. Policy Ownership and Responsibility

The policy is owned by the **74Software** Executive Committee.

AI governance is complementary to other governance processes and policies of relevant functions in 74Software who work collaboratively to manage AI risks (e.g. Compliance, Security, Procurement teams, etc).

All Colleagues granted access to 74Software devices and networks are responsible for reading, understanding, and adhering to this policy.

4. AI Business Principles

There are 5 key principles we should adhere to when we develop AI systems, so we can be confident our deliveries align to the overall Business goals, Strategy and Security Expectations.

They are:

Solve **DEFINED PROBLEMS**	Identify requirements where AI techniques are well matched to desired outcomes. AI may supplement what we already do and does not have to replace it

Provide **CLEAR VALUE**	We need a clear path and understanding of the specific value that an AI development will provide. Are the outcomes valuable to 74Software and our Clients?
Implement **ETHICALLY & SECURELY**	Use Data & Tooling in line with our values. Understand any exposure or risks we may face from the developments we undertake.
Ensure **EXPLAINABILITY**	We must control our AI rather than it controlling us. With the ability to explain and the confidence to stand behind our outputs.
Maximise **RE-USABILITY**	Ensure that AI initiatives are produced in a way that can be re-used within other areas. To make sure we don't need to recreate the wheel.

These should be considered at all stages of the AI development cycle from selecting use cases to delivery, and as principles will help guide our actions in addition to the rest of the AI Policy & AI Standards.

5. Policy Requirements

5.1 Approval of AI Tools

AI tools need to be approved for use in accordance with the processes defined in the 74Software AI Standards and may not be used without an appropriate risk assessment being completed. AI tools which are approved for certain use cases may not be used for unapproved use cases. For example, if an AI tool is approved for internal use to create internal documents and presentations, it may not be used for materials developed for use by clients, partners or other external purposes without a further approval being obtained. This is to ensure that the specific risks associated with AI use are assessed and mitigated e.g. to guard against intellectual property leakage, data privacy, confidentiality or security breaches and the misuse of AI or its output.

Use of AI should be approved on a case-by-case basis, and an approval cannot be considered general approval.

It is also a requirement under the 74Software IT use policy that only approved software tools are used in the organization and Colleagues are reminded that they are not permitted to download and install unapproved AI tools and models on their 74Software issued devices or on personal devices used with or for 74Software related data.

Through risk assessment, new use cases for AI tools may be categorized based on the use case or nature of the data processed – e.g. high, medium, low risk. Details of this can be found in the AI Governance Policy.

Records will be kept of AI tools approved for use in accordance with applicable regulatory requirements.

We recognize that Colleagues may want to use certain online AI tools (such as ChatGPT and OpenAI) for their own administrative or research purposes, in the same way free tools such as Google search may have been used. These tools must be used in line with AI Tooling Standards (e.g. For personal use and internal purposes only, with no confidential, proprietary or personal data from 74Software and any 74Software Entities, or any third party) and if used for any related work activity a 74Software account should be used.

5.2 Use of AI in Product Development

Development of AI in 74Software products and offerings must follow 74Software's established product governance processes. Additional 74Software governance processes and design requirements specific to AI and designed for development of responsible AI must also be followed.

5.3 Procurement and Supplier Management

Procurement of third-party AI tools are subject to the standard procurement process and additional checks and due diligence to be completed by suppliers for an understanding of the tool and so that risk assessments can be undertaken by the appropriate teams (e.g. technical, legal, compliance and security).

Many suppliers are building AI add-on features into their existing software products, and it may not be immediately obvious that these contain AI. Our processes are designed to check if this is the case and existing suppliers which incorporate AI in their offerings will also be asked to complete AI due diligence assessments.

If an AI feature/add-on has not been approved for use, then disable/do not use the AI feature/add on.

5.4 Human Insight and Risk Mitigation

AI deployed at 74Software should be monitored for reliability to detect any issues.

Human oversight of AI decisions will be required where this is necessary based on the context e.g. content created by AI needs to be checked carefully by Colleagues for errors and cannot be assumed to be accurate or appropriate for use. The output should be carefully reviewed together with other relevant information, and decisions should not be based solely on the output of the AI tool. Internal tools (e.g. Threat Modeling, SCA, SAST, DAST, Container Scanning, etc.) should be used whenever possible.

Colleagues will be accountable for their use of AI tools, the input provided, and the output used by them.

5.5 Transparency

Users or those impacted using AI tools must be informed of the use of AI in line with any transparency requirements under applicable regulation such as interaction with an AI Chatbot or an AI that plays a significant role in decisions that may affect them. This means, for example, if an AI Chatbot is in use, we must clearly disclose that AI is used in the user interface or documentation or if an AI feature is built into a product, this should be communicated in an unambiguous way. 74Software is committed to providing clear, accurate, and accessible information to clients regarding the use of AI in its products and services. 74Software must ensure that customers are informed when AI is embedded in solutions they use, including the nature of AI functionalities, associated risks, and 74Software safeguards in place. 74Software will respond transparently to customers' inquiries and ensure accountability through dedicated governance channels.

5.6 AI Literacy, Training and Enablement

Training and enablement for use of AI will be provided where needed for correct use of AI by 74Software and its Entities.

Where relevant to the tool, Colleagues will also be trained on issues related to AI generated content to understand how to mitigate risks e.g. risks posed by bias, errors in content produced, IP risks.

Colleagues are expected to complete relevant AI training and literacy programs offered by 74Software to promote an understanding of this emerging technology and its safe adoption.

Due to the nature of AI and its range of associated risks, specific organizational functions are responsible for identifying additional training needs for their use cases and for training AI users within their function.

5.7 Incidents and Issues Encountered

Any incidents, material issues or errors encountered by Colleagues using an approved AI tool should be reported immediately through the appropriate channel within 74Software. Additionally, if you think confidential or personal data has been submitted to a tool which should not have been this should also be reported immediately.

5.8 Legal Compliance

74Software will maintain a Governance Framework and Standards for managing AI and will apply for relevant certifications for AI where this is required under applicable law.

The release of a product or a SaaS service including AI features must be compliant with the regulations where 74SW operates. Compliance is verified by the AI Steering Committee.

AI tooling must not be used for any prohibited uses under any regulation. Examples from the EU AI Act can be seen in Annex 1.

Human Rights Impact Assessments requirements for High-Risk AI will be undertaken where required under applicable law.

5.9 Intellectual Property

74Software and 74Software employees using AI must ensure that the use, development, and deployment of AI systems respect and protect intellectual property rights. AI tools and outputs must not infringe third-party IP and must not incorporate externally sourced material unless proper rights have been obtained. 74Software employees must refrain from exposing 74Software proprietary algorithms, data, information, source code, or confidential designs to any AI platform, especially external or open tools.

5.10 Data Privacy and Protection

All AI related activities must comply with applicable data protection laws, including the GDPR. Personal data of customers, employees, or third parties must not be processed by AI systems without a valid legal basis, consent and documented safeguards. Use of AI tools must be aligned with 74Software privacy policies and must undergo data protection impact assessments (DPIAs) where appropriate.

5.11 Sensitive and Confidential Information

AI systems must not be trained or operated using sensitive or confidential business information belonging to 74Software or any of its employees or customers, unless explicit authorization and adequate safeguards

are in place. Particular caution must be taken to prevent exposure of client data, business strategies, financial information, or sensitive operational metrics.

5.12 Environmental Impact

When selecting, developing, or deploying AI solutions, consideration must be given to their energy consumption and computational efficiency. Preference will be given to models and infrastructure aligned with 74Software sustainability goals to acknowledge and manage the potential carbon footprint of AI solutions in line with 74Software's sustainability commitments.

5.13 Policy Violations

Violations of the provisions of the policy or standards of acceptable use by Colleagues may be subject to the following actions:

- Investigation of any breaches or events leading to violation.
- Relevant disciplinary action.
- Removal of access to 74Software and its Entities facilities, networks and systems.

5.14 Policy Review Cadence

This policy will be reviewed annually but may additionally be updated on an ad hoc basis to account for changes in Strategy, Regulation or other relevant Business need.

6. Related Documents & Associated Policies

Below are the policies and standards assocaited with this policy.

Please see the standards:

- AI Governance Framework and Standards

For further information in the below areas please refer to the relevant policies which should be adhered to in association with this Policy:

Secure Data Handling Policy
Records Management Policy
Risk Assessment Policy
IT and OEM Supplier Management Policy

Annex 1 EU AI ACT Prohibited Use Cases

Article 5(1)(c)	Social scoring	AI systems that evaluate or classify natural persons or groups of persons based on social behaviour or personal or personality characteristics, with the social score leading to detrimental or unfavourable treatment when data comes from unrelated social contexts or such treatment is unjustified or disproportionate to the social behaviour
Article 5(1)(d)	Individual criminal offence risk assessment and prediction	AI systems that assess or predict the risk of people committing a criminal offence based solely on profiling or personality traits and characteristics; except to support a human assessment based on objective and verifiable facts directly linked to a criminal activity
Article 5(1)(e)	Untargeted scraping to develop facial recognition databases	AI systems that create or expand facial recognition databases through untargeted scraping of facial images from the internet or closed-circuit television ('CCTV') footage
Article 5(1)(f)	Emotion recognition	AI systems that infer emotions at the workplace or in education institutions; except for medical or safety reasons
Article 5(1)(g)	Biometric categorisation	AI systems that categorise people based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex-life or sexual orientation; except for labelling or filtering of lawfully acquired biometric datasets, including in the area of law enforcement
Article 5(1)(h)	Real-time remote biometric identification ('RBI')	AI systems for real-time remote biometric identification in publicly accessible spaces for the purposes of law enforcement; except if necessary for the targeted search of specific victims, the prevention of specific threats including terrorist attacks, or the search of suspects of specific offences (further procedural requirements, including for authorisation, outlined in Article 5(2-7) AI Act).