



TECHNICAL ALERT 01/2025

Pointers for a firm's Artificial Intelligence policy

This publication has been jointly developed by the member bodies of the Consultative Committee of Accountancy Bodies – Ireland (CCAB-I), being the Institute of Chartered Accountants in Ireland and the Association of Chartered Certified Accountants (ACCA).

February 2025

Disclaimer

This publication has been jointly developed by the member bodies of the Consultative Committee of Accountancy Bodies – Ireland (CCAB-I), being the Institute of Chartered Accountants in Ireland and the Association of Chartered Certified Accountants (ACCA).

The content of this publication is provided as a guide only and does not purport to give professional advice. It should, accordingly, not be relied upon as such. No party should act or refrain from acting on the basis of any material contained in this publication without seeking appropriate professional advice. While every reasonable care has been taken by the member bodies of the Consultative Committee of Accountancy Bodies - Ireland (CCAB-I) in the preparation of this publication we do not guarantee the accuracy or veracity of any information or opinion, or the appropriateness, suitability or applicability of any practice or procedure contained therein. The member bodies of the CCAB-I are not responsible for any errors or omissions or for the results obtained from the use of the information contained in this publication.

To the fullest extent permitted by applicable law, the member bodies of the CCAB-I exclude all liability for any damage, costs, claims or loss of any nature, including but not limited to indirect or consequential loss or damage, loss of business profits or contracts, business interruption, loss of revenue or income, loss of business opportunity, goodwill or reputation, or loss of use of money or anticipated saving, loss of information or loss, damage to or corruption of data, whether arising from the negligence, breach of contract or otherwise of the member bodies of the CCAB-I, their committee members, employees, servants or agents, or of the authors who contributed to the text, even if advised of the possibility of such damages.

Similarly, to the fullest extent permitted by applicable law, the member bodies of the CCAB-I shall not be liable for any indirect or consequential losses including but not limited to, loss of business profits or contracts, business interruption, loss of revenue, loss of business opportunity, goodwill or reputation, or loss of use of money or anticipated saving, loss of information or damage to or corruption of data, nor shall it be liable for any damage, costs or losses of any nature (whether direct or indirect) occasioned by actions, or failure to act, by users of this publication or by any third party, in reliance upon the contents of this publication, which result in damages or losses incurred either by users of this publication, for whom they act as agents, those who rely upon them for advice, or any third party, or for any breach of contract by

the member bodies of the CCAB-I in respect of any inaccurate, mistaken or negligent misstatement or omission contained in this publication.

All rights reserved. No part of this publication is permitted to be reproduced for resale, stored in a retrieval system for resale, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise for resale, or for any other purpose, without the prior and express written permission of the copyright holder. Nor is any right granted for any part of this publication to be copied or otherwise used in any presentation or training course without the prior and express written permission of the copyright holder. For professional advice on any of the matters referred to above, please contact the relevant member body of the CCAB-I.

Any issues arising out of the above will be governed by and construed in accordance with the laws of Ireland and the courts of Ireland shall have exclusive jurisdiction to deal with all such issues.

© Institute of Chartered Accountants in Ireland, Association of Chartered Certified Accountants,
2025

Introduction

Most readers will already have encountered the words artificial intelligence or AI. Examples of AI tools are large language models (LLMs), plug ins, data enabled AI tools, Chat GPT, DALL-E, and Codex.

If you are a business, your employees may already be using some form of artificial intelligence as a trial to test it out or even to assist them in their work. AI can help businesses to increase efficiency, for instance by automating repetitive tasks. However, you may not, for example, want a bot (short for robot or an automated program) to attend or record a confidential meeting.

This technical alert is not a silver bullet considering everything the reader should include in an AI policy, but we hope it might give some pointers or ideas on what to look out for if your business is using AI and to inform your staff on what is allowed in terms of using AI in their role.

Practical suggestions

We would suggest that businesses should have a policy in place in respect of the use of AI in the workplace. Everyone in your workplace should know what is and is not permitted. They should have an awareness and understanding of the benefits, risks, safeguards, rights and obligations in relation to the use of AI systems and the responsible use of AI.

An AI usage policy should be reviewed in conjunction with your other policies such as those on Data Protection, IT, Cybersecurity and Risk related policies and you should be cognisant of publications and guides such as those listed under Useful resources below.

AI systems should be designed and operated to avoid, mitigate or eradicate unfairness or bias, ensuring that decisions are justified, non-discriminatory and transparent, and that there is no output that could constitute harassment. Users must ensure that there is always a human in the loop for critical decisions made by AI. See below under “Ethical use and limitations”.

In creating your AI policy, you should also include standard clauses suitable for any policy such as its purpose objective and scope. This technical alert has not considered other elements such as AI system development and deployment, third party management and governance structure outlining oversight roles, and assigned responsibilities. All of these should be considered on a case-by-case basis depending on circumstances.

Every staff member should be required to sign up for the AI policy.

Use of AI-General considerations

- Use of AI by employees and others in the business - whether you permit “free to use” software or not.
- A ban on any use of high-risk models and engaging in prohibited AI practices
- Evaluation of tool security before use
- Request and approval for each tool should be sought by employees before use
- Use of permitted tools and models approved by IT only
- “Permitted use” by “permitted user” only
- A ban on the use of personal or third-party devices for company business/work related purposes
- Confidentiality – any data inputted must not breach any duty of confidentiality

Compliance with law

- You must comply with the AI Act and any other AI legislation, data protection, intellectual property, privacy/confidential information and anti-discrimination laws.
- Data handling and management must be in accordance with data protection law.
- There must be a prohibition on using personal or sensitive data in AI systems.
- Be mindful of AI that is open source where information or data fed in becomes public and could lead to or permit information sharing with external parties, directly or indirectly.
- AI users must ensure any data used for AI is accurate, relevant, and up to date.

Ethical use and limitations

- There must be recognition of AI limitations
- Be aware of the phenomenon of “hallucination” where AI models generate outputs that are nonsensical or inaccurate
- Human judgment must be applied to AI output
- There must be human oversight and accountability
- Reliance on output -there must be independent verification of outcomes, fact checking, the ability to explain and justify conclusions/outcomes, external sources
- Consider if prior approval should be required for use of AI output outside the organisation
- Where relevant, consider a disclaimer that content has been generated by AI
- You must provide staff training on responsible AI use and appropriate foundational legal and AI training must also be provided
- Ethical implications must be considered

Plan for misuse/malfunction [governance, audits and compliance management]

- Use monitoring and compliance must apply and regular audits must occur
- Have risk and risk control mechanisms in place for risk level of incidents to be assessed
- Make a disaster plan for misuse/malfunction of AI technologies
- Set up a mechanism for incident management, reporting of incidents (including timeline) and response to incidents
- Resources (personnel and financial) must be available to deal with misuse /malfunction of AI

Useful resources

[Irish Data Protection Commission Data controllers' guide](#)

[First EDPS Orientations for EUIs using Generative AI | European Data Protection Supervisor \(europa.eu\)](#)

[National AI Strategy Refresh 2024](#)