

Guidance on Digital Ethics

This guidance is to be used by members as a supplementary reference alongside the CISI Code of Conduct. It specifically focuses on the ethical principles for consideration within digitalisation and changing technologies.

Technologies offer significant opportunities to make our lives easier, safer, more comfortable, efficient and fun. They also present a range of risks that may impact people's privacy and their trust in these technologies, if they are not addressed as the technology develops.

This guidance is structured into two distinct parts: one focusing on ethical considerations for technology developers, and the other tailored for users.

Each section provides detailed guidance complemented by illustrative scenarios.

TECHNOLOGY DEVELOPERS

Responsible use of technology



Members must ensure that data is handled responsibly, with transparency and in accordance with applicable laws and regulations.

Members should also make sure that technology is used ethically, complying with the expected professional code.

Members should ensure that technology is used for the purpose for which it was designed, and any changes should be implemented through a change management function.

Can you identify where the data originates from?

Has the data been altered in any way?

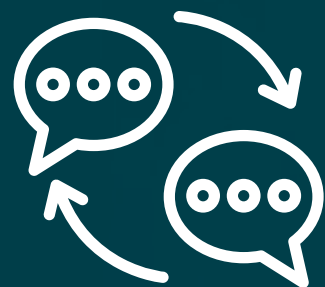
Does everyone understand their responsibility when using technology or AI systems?

Has the firm taken steps to safeguard client confidentiality, ensuring that personal or private information is not fed into AI systems such as ChatGPT?

Example scenarios

Ensuring sensitive personal information is not input into AI generators, and that staff are aware of what new AI systems and technologies are, their limitations and what they are capable of.

Interpretability



Members must ensure that the recommendations/suggestions generated by AI are logical and can be explained and interpreted.

Is it possible to explain the decisions and predictions generated by technology or AI systems?

How easy would it be to replicate the suggestions generated and explain these to clients/public?

Example scenarios

Ensuring that team leaders can correctly explain how decisions for the AI systems are made.

TECHNOLOGY DEVELOPERS

Privacy and consent



Personal information may be collected by technologies that may not be transparent to the public.

Some data ecosystems may make it difficult for people to understand how organisations are processing their information and hold them to account.

Obtain correct permissions when using intellectual property.

Ensure credit is given when sharing digital content.

Consider the accuracy of your data and the legal consequences of entering data in technology.

How easy is it for individuals to manage their data, and how may it be reused in the future?

How can you best educate teams to ensure they avoid entering any personal, private, or sensitive information into data systems?

Example scenarios

Making it easy for individuals to request and manage their personal data and preferences on a firm's website.

Avoid inputting client information or similar information into ChatGPT to produce an outcome for your request. This could lead to data privacy and legal breaches.

Feedback and learning



Be open to feedback on technological developments from users and stakeholders to improve best practice.

How easy is it to speak up and raise a concern?

How easy it is to provide feedback on what is working well and what could be improved?

Example scenarios

Putting customer needs first. One way is by ensuring a website easily indicates where you can provide feedback, and where you can raise a concern.

TECHNOLOGY DEVELOPERS

Risk and compliance



Many technologies are collecting information about sensitive personal characteristics that may require additional safeguards.

It is important to ensure regular risk assessments are carried out to safeguard data from unauthorised access, use or disclosure, testing these measures where appropriate and ensuring that everyone understands them.

How reliable and robust is the AI system?

How can you ensure that clients and firms are not exploited using AI systems?

Example scenarios

Ensuring that teams understand the importance of regularly changing their passwords for devices.

Bias



Being aware of biases created by technologies and heightened risks to certain groups.

Confirmation bias – this can be demonstrated in the way the prompt is written to which generative AI will develop a response.

The halo effect – how can you mitigate AI systems from focusing solely on one feature about a particular issue/event?

Have you considered the various types of bias and how they can be mitigated?

Example scenarios

Ensure that applications utilising client data fully leverage the diverse range of information available. Where apps use client information to help determine financial product marketing.

Fairness



AI systems should be fair and accessible to all. They should consider data from all stakeholders with their various needs.

Have you ensured that the development of your AI system uses inclusive data and is without favouritism or discrimination?

Example scenarios

An AI system using representative and diverse data when providing solutions to firms.

Use of social media



Considering how you use your social media account and what impact this may have on your professional network.

Ensuring accuracy and reliability of information and its sources, before sharing what can be false or misleading content online.

Refraining from engaging in any form of online harassment and reporting inappropriate behaviour.

How are you using your social media account?

Example scenarios

Avoiding contributing to a social media account, which promotes online harassment.

Refraining from re-sharing a social media post on how investing in certain products could transfer into fast capital gains.

Refraining from contributing to an online webinar, where the chat function has turned into harassment of the panellist.

References:

AAT, Ethics guidance note, Digital Ethics:

www.aat.org.uk/prod/s3fs-public/assets/AAT-ethics-guidance-note-Digital-ethics.pdf

ACCA Ethics and Trust in a Digital Age:

<https://www.accaglobal.com/gb/en/technical-activities/technical-resources-search/2017/august/ethics-and-trust-in-a-digital-age.html>

AICPA, Making good decisions: building trust in a digital world. The ethics of new technology and how to act:

<https://insights.cgma.org/story/ethics-of-new-technology/page/1?teaser=true&vngagetrans=Q57DUAugMOG4mu4neXgL>

CII Digital Ethics Companion:

<https://www.cii.co.uk/about-us/professional-standards/code-of-ethics/>

Gov.UK 'Safer platform checklist: practical steps to protect your users from online harms':

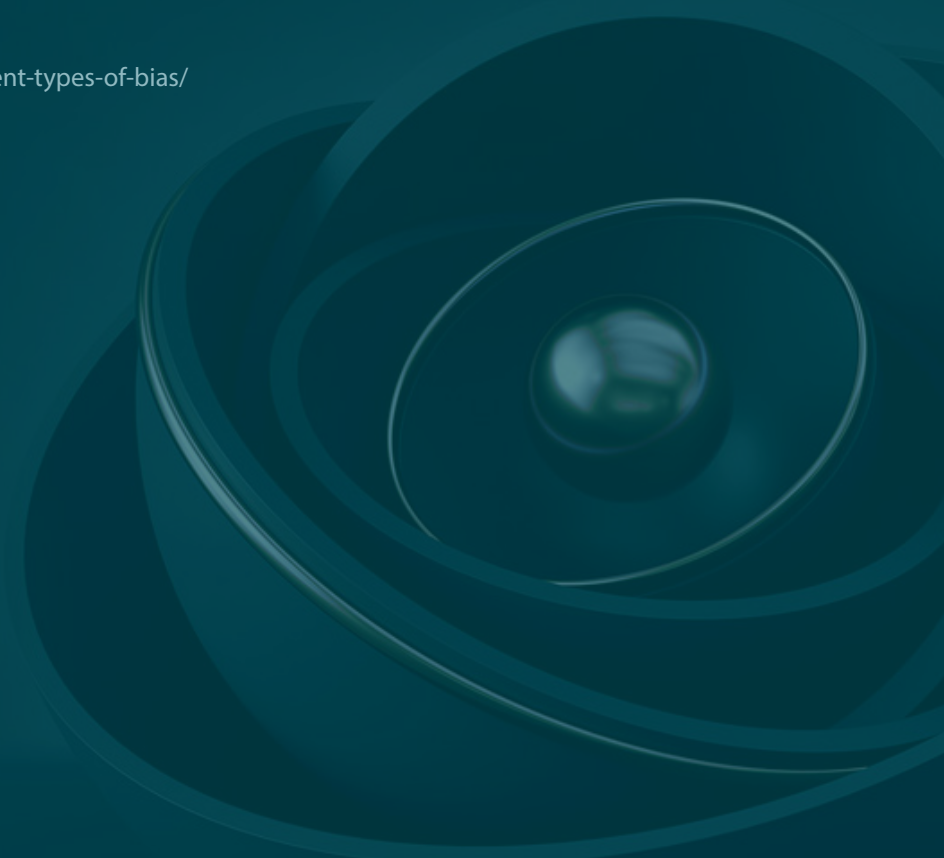
<https://www.gov.uk/guidance/safer-platform-checklist-practical-steps-to-protect-your-users-from-online-harms>

ICO Tech Horizons Report – December 2022:

<https://ico.org.uk/about-the-ico/research-and-reports/tech-horizons-report/>

National School of Healthcare Science, NHS England, October 2022 :

<https://nshcs.hee.nhs.uk/about/equality-diversity-and-inclusion/conscious-inclusion/understanding-different-types-of-bias/>





Certificate in Ethical Artificial Intelligence (AI)

A short online course with tests and a certificate involving 12 hours of learning

As AI becomes more advanced and widespread, there are growing concerns about issues such as bias, transparency, accountability, and safety. If you're in search of a jargon-busting course that not only delves into the core definitions and global developments in the field of AI but also explores its ethical dilemmas and what they mean for financial services, as well as the responses of regulators, this new certificate offers an outstanding overview. This short course, involving 12 hours of online study, is essential learning for anyone wanting to understand the fundamental ethical and management issues in the deployment of AI in finance.

Key features

- Short course of online self-learning with a certificate when you pass
- Understand the key terminology and issues
- Enhance your employability by demonstrating your competence
- Written by experts for financial services practitioners
- Covers all the fundamental information needed by professionals
- Global perspective and overview of an essential subject
- Can be taken anytime and anywhere on any device
- 12 hours of CPD

Members £60

The course for members comprises four mandatory modules with online tests (8 hours total) and an additional 4 hours of flexible CPD in AI learning via the CISI Learning Platform

- Ethical AI and Professional Codes of Conduct
- Risk Management in AI
- Strategic Approaches to AI
- Tactical Development of AI (Executive Management)
- Additional four hours of flexible CPD in AI Learning via the CISI Learning Platform

Non-members £150

The non-member course comprises five mandatory modules with online tests (10 hours) and a further module of curated AI learning (2 hours) for a total of 12 hours of learning.

- AI - an introduction
- Ethical AI and Professional Codes of Conduct
- Risk Management in AI
- Strategic Approaches to AI
- Tactical Development of AI (Executive Management)
- Further module containing curated AI learning (videos/articles)

