Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

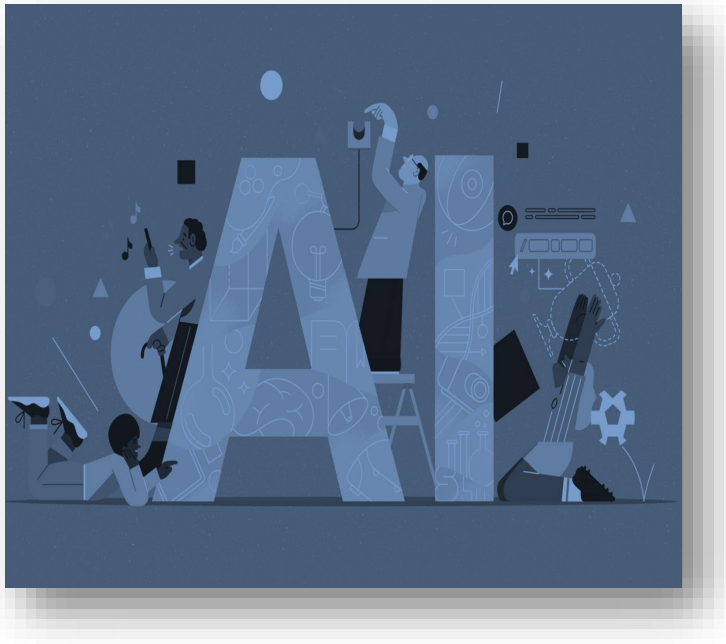
GenAI & GDPR

tcd.ie/dataprotection

What is an “AI system”?

A machine-based system 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

Different AI systems vary in their levels of autonomy and adaptiveness after deployment



What is “Generative AI / GenAI”?

An AI model which is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications

Responsibilities for Users of AI systems

1. Protect data

   - Do not enter data classified as "*University Internal*", "*Restricted*" or "*Critical* " into publicly-available GenAI software

   - There is no guarantee that information inputted into external AI tools will remain confidential. Information shared with AI tools using default settings is not private and could expose information to unauthorised parties and result in a data breach

   - The University data classification chart is available at https://www.tcd.ie/itservices/keeping-it-secure/data-classification/

Responsibilities for Users of AI systems

2. Purchasing / Using AI software

- If you are considering purchasing or using a licence (paid-for or free version) for an AI tool to process University-controlled data for educational, research or operational purposes you must contact IT Services and the Data Protection Officer to complete an assessment of the proposed software solution

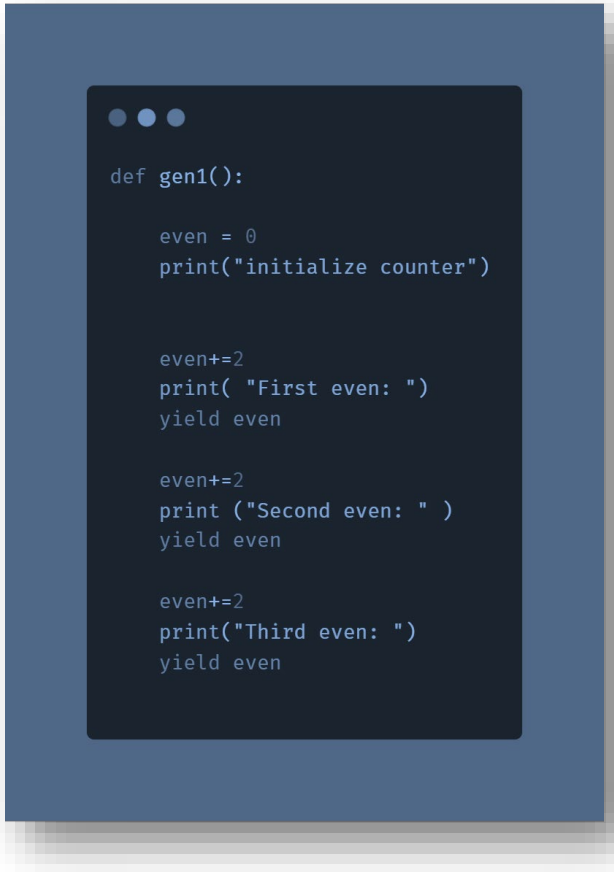
itservicedesk@tcd.ie

dataprotection@tcd.ie

Responsibilities for Users of AI systems

3. Code generation

- GenAI tools should not be used to produce code as they can create software/code that has security vulnerabilities, bugs and uses illegal libraries or calls
- Any code written with the assistance of an AI tool should be reviewed by a human developer trained in that programming language



Responsibilities for Users of AI systems

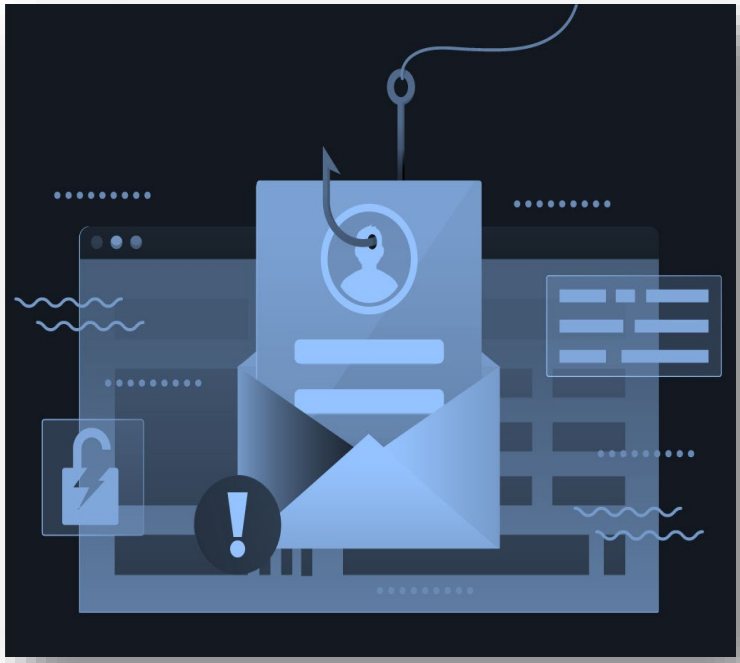
4. Content generation

- Content generated by AI can include copyrighted material, inaccurate or misleading information or can sometimes be entirely fabricated
- Review any AI generated content before publication as you may be responsible for infringements or errors in the material

Responsibilities for Users of AI systems

5. Stay alert

- Phishing has become more sophisticated due to AI
- With AI phishing, cyber criminals use AI tools to correct poor grammar, remove spelling mistakes and add idiosyncrasies to sound more like a native speaker, luring victims into a false sense of security



Responsibilities for Users of AI systems

6. Use your judgment

- Always use your professional judgement when using AI to process Trinity data
- Do not assume that AI outputs are accurate - review outputs to ensure accuracy and alignment with the College's vision and values
- Avoid free AI tools which can lack security measures and may result in disclosure of proprietary information

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

tcd.ie/dataprotection