Department of Finance
An Roinn Airgeadais
www.finance-ni.gov.uk

NICS
Use of Generative AI Policy

DOCUMENT CONTROL

The Department of Finance Shared Services Chief Information Security Officer is the owner of this document and is responsible for ensuring it's distribution. The document will be reviewed annually.

DOCUMENT INFORMATION

Title	NICS Use of Generative AI – Policy	**Version**	2
Author	[redacted]	**Date**	30/05/2023
Reviewed By	[redacted]	**Date**	07/06/2023
Approved by	[redacted]	**Date**	07/06/2023
TRIM Reference	[redacted]	**Review Date**	07/06/2025

CHANGE HISTORY

Ver. No.	Ver. Date	Revised By	Description	Reviewer	Status
2	05/06/2024	[redacted]	Ownership updated	[redacted]	Approved
2	05/06/2024	[redacted]	Reference to the AI Cyber Security	[redacted]	Approved
2	05/06/2024	[redacted]	Sequence of approvals updated.	[redacted]	Approved

DISTRIBUTION

Group	Date
[redacted]	11 June 2024
[redacted]	11 June 2024
[redacted]	11 June 2024
[redacted]	11 June 2024

Contents

Document Control 2

1 Introduction 4

1.1 AIM 4

2 Strategic Context 4

3 Generative AI 4

3.1 Generative AI 4

3.2 Ethical Implications 5

3.3 Benefits 5

4 UK AI Regulatory Framework 5

5 AI CYBER SECURITY CODE OF PRACTICE 6

6 Use of Generative AI within NICS 6

7 Appendix 1 - Glossary 8

8 Appendix 2 – Useful Links 9

1 INTRODUCTION

1.1 AIM

The aim of this policy is to ensure a consistent approach on the use of Generative AI across the NICS.

2 STRATEGIC CONTEXT

The National AI Strategy, published in September 2021 stated that *'the UK has an opportunity over the next ten years to position itself as the best place to live and work with AI; with clear rules, applied ethical principles and a pro-innovation regulatory environment. With the right ingredients in place, we will be both a genuine innovation powerhouse and the most supportive business environment in the world, where we cooperate on using AI for good, advocate for international standards that reflect our values, and defend against the malign use of AI'.*

Effective, pro-innovation governance of AI means that:

(i) the UK has a clear, proportionate and effective framework for regulating AI that supports innovation while addressing actual risks and harms,

(ii) UK regulators have the flexibility and capabilities to respond effectively to the challenges of AI,

(iii) organisations can confidently innovate and adopt AI technologies with the right tools and infrastructure to address AI risks and harms.

The strategy highlighted that the UK public sector will lead the way by setting an example for the safe and ethical deployment of AI through how it governs its own use of the technology.

3 GENERATIVE AI

3.1 GENERATIVE AI

Generative AI is a broad label used to describe any type of artificial intelligence (AI) that can be used to create new text, images, video, audio, or code. Large Language Models (LLMs) are part of this category of AI and produce text outputs.

ChatGPT is an example of a Generative AI language model. ChatGPT was developed by OpenAI, based on the GPT (Generative Pre-trained Transformer) architecture. ChatGPT is trained on a massive dataset of text from the internet, including books, articles, and websites, and it uses deep

learning techniques to generate responses that are contextually relevant and grammatically correct. It can be used for a variety of natural language processing tasks, such as language translation, summarization, and conversation generation.

3.2 ETHICAL IMPLICATIONS

With all AI technologies, there are concerns about the ethical implications of AI use, particularly in areas such as bias, privacy, and the potential for misuse. As such, responsible use of AI, along with appropriate regulation and oversight, is essential to ensure that it is used for good and benefits society as a whole.

3.3 BENEFITS

NICS recognises the potential benefits of using artificial intelligence (AI) to improve efficiency and productivity in the workplace. However, we also acknowledge the importance of using AI responsibly and ethically, particularly when it comes to generating content.

4 UK AI REGULATORY FRAMEWORK

While AI is currently regulated through existing legal frameworks like financial services regulation some AI risks arise across, or in the gaps between, existing regulatory remits. Department for Science, Innovation and Technology (DSIT) recognise Government intervention is needed to improve the regulatory landscape and published a policy paper 'A pro-innovation approach to AI regulation' on 29 March 2023.

The intention is to support innovation while providing a framework to ensure risks are identified and addressed using a proportionate and pro-innovation regulatory framework. Rather than target specific technologies, it focuses on the context in which AI is deployed. This enables a balanced approach to weighing up the benefits versus the potential risks.

Regulating the use – not the technology – the proposed framework is context-specific. It will not assign rules or risk levels to entire sectors or technologies, it will regulate based on the outcomes AI is likely to generate in particular applications.

5 AI CYBER SECURITY CODE OF PRACTICE

As with any technology, the continued evolution and uptake of AI will also present challenges. To address these challenges, the government set out its pro-innovation and pro-safety regulatory framework, which will ensure that we are able to maximise the opportunities and minimise the risks of this fast-moving technology. The AI regulation white paper outlined five cross-sectoral principles to be applied by existing UK regulators, and a new central function to bring coherence and address regulatory gaps.

It is the Government's intention, to submit an updated voluntary Code of Practice to the European Telecommunications Standards Institute (ETSI) in September 2024 to help inform the development of this global standard on baseline cyber security for AI systems and models.

The Code sets out practical steps for stakeholders across the AI supply chain, particularly Developers and System Operators, to protect end-users. The Code applies to all AI technologies and will help ensure that security is effectively built into AI models and systems as well as across the AI lifecycle. It is important for stakeholders to note that this voluntary Code sits in support of the UK Government's wider efforts for AI and regulations, such as UK data protection law. Users of Generative AI Models must ensure the solution they are utilising complies with the proposed Code of Practice Principles and any future iterations.

https://www.gov.uk/government/calls-for-evidence/call-for-views-on-the-cyber-security-of-ai/call-for-views-on-the-cyber-security-of-ai

6 USE OF GENERATIVE AI WITHIN NICS

NICS Departments are committed to identifying and capturing opportunities arising from emerging technologies. Business areas can research and find out more about Generative AI technologies, expand their understanding of how they can be used, how they work, and ensure they are used in a safe and ethical manner. For all new technologies, it is important to be both aware of risks, but alive to the opportunities they offer.

Aligning with the wider UK approach, but acknowledging the current absence of a fully developed Regulatory Framework, NICS staff wishing to utilise the technology must;

- Receive approval (Grade 6 minimum approval grade) for the specific use case(s) in which they intend to use AI;
- Engage with the Departmental ITSO and provide the SIRO with written assurance that a security assessment has been carried out and the Generative AI Model aligns with the principles detailed within the AI Cyber Security Code of Practice, NCSC guidance 'Principles for the security of machine learning', 'securing your infrastructure' and 'data supply chains' that there is no risk to NICS;
- Engage with the DPO to ensure a full understanding of the terms of use and privacy notice of the Generative AI Model they intend to use. Consider a Data Protection Impact

Assessment to ensure compliance with UK Data Protection legislation and that there is low/no risk to personal data.

- Receive approval from the Departmental Senior Information Risk Owner for the specific use case(s) in which they intend to use AI;
- Adhere to the guidance on 'The use of Generative AI in the NICS – Guidance Paper'
- Provide assurance to, the G6 (minimum), DPO and ITSO and SIRO during and on completion of the Generative AI usage that all data, privacy, information, security and ethical regulations / standards have been adhered to.

7 APPENDIX 1 - GLOSSARY

AI	Artificial Intelligence
DPO	Data Protection Officer
DSIT	Department for Science, Innovation and Technology
GPT	Generative Pre-trained Transformer
ITSO	IT Security Officer
LLM	Large Language Models
NCSC	National Cyber Security Centre
NICS	Northern Ireland Civil Service
SRIO	Senior Information Risk Owner

8 APPENDIX 2 – USEFUL LINKS

AI regulation: a pro-innovation approach - GOV.UK (www.gov.uk)

National AI Strategy - GOV.UK (www.gov.uk)

Principles for the security of machine learning - NCSC.GOV.UK

Secure your infrastructure - NCSC.GOV.UK

Supply chain security guidance - NCSC.GOV.UK