Ofcom's strategic approach to AI 2024/25

Ofcom's strategic approach to AI 2024/25 – Welsh version

Publication date: 26 March 2024

Contents

Section

Annex

1. Introduction

1.1 **Ofcom is the UK's communications regulator**, with functions across fixed and mobile telecoms, post, spectrum, TV and radio broadcasting, UK-established on-demand services and video sharing platforms. Ofcom is also the UK's online safety regulator under the Online Safety Act 2023 (OSA)[1], and has duties including in media literacy, telecoms security and news media plurality. At the core of Ofcom's mission is our commitment to make communications work for everyone in the UK. As a converged regulator, we work across our responsibilities to achieve our four priority outcomes, around which our Plan of Work 2024/25 is centred**:**

a) Internet we can rely on,

b) Media we trust and value,

c) We live a safer life online, and

d) Enabling wireless services in the broader economy.

1.2 **The use of artificial intelligence (AI) in the sectors we regulate is not new, but recent innovations have seen widespread adoption of AI to create content.** AI has been around for decades, evolving from early algorithms capable of performing simple tasks in the 1980s to the sophisticated systems of today that are transforming society, business processes, and consumer experiences. The AI transformation has been powered by a wide array of key technologies – including machine learning (ML)[2], natural language processing (NLP)[3], computer vision[4], and speech recognition[5] – redefining the limits of what machines can do. While more advanced forms of AI have been in development for some time, in the past year the mainstream emergence and adoption of Generative AI (GenAI) marks a pivotal leap forward in AI, given its ability to generate new content (text, images, video and audio) seemingly mimicking human creativity and intelligence at an unprecedented scale.

1.3 **These technologies are spurring innovation with the potential to offer substantial benefits for businesses and consumers in the communications and media sectors.** AI already powers search, social media, and messaging services online. Network operators are using AI to enhance network planning, optimise the building of networks, and detect and prevent fraudulent behaviour. Looking forward, advancements in GenAI offer profound opportunities. In online safety, GenAI could be used to create new datasets to improve the accuracy of online safety technologies.[6] In the broadcasting sector, GenAI can be used to create more compelling visual effects in TV production. Similarly, for comms services, GenAI can be used by mobile and messaging providers to detect and filter spam and unwanted messages more effectively.

---

[1] Online Safety Act 2023

[2] Machine learning uses algorithms trained on data sets to create models that allow machines to perform more complicated tasks usually performed by people, such as categorising images and analysing data

[3] Natural language processing allows computers and other devices to recognise, understand and generate text and speech

[4] Computer vision teaches computers and systems to analyse digital images, videos and other visual inputs.

[5] Speech recognition enables a computer programme to process human speech into a written format

[6] What generative AI means for the communications sector (June 2023)

1.4 **However, these advancements also pose challenges and risks which need to be addressed.** For example, GenAI can be used to create illegal or harmful content which can spread quickly online, such as deepfake[7] pornography or instructions for self-harm. GenAI models can also be used by malicious actors to create 'fake' content including news and media, increasing the risk of mis- and disinformation for consumers. Elsewhere, GenAI can also be used to create more sophisticated fraud and scams, for example by mimicking the voice of loved ones over the phone or by creating more convincing phishing content online.

1.5 **As AI technologies continue to develop at pace, we look to harness the benefits while mitigating risks in line with the Government's pro-innovation approach to AI.**[8] Ofcom is supportive of the Government's AI principles (see Figure 1) as a useful lens through which to consider our work on AI. These principles – safety, security and robustness; appropriate transparency and explainability; fairness; accountability and governance; and contestability and redress – are broadly aligned with the underlying principles of our regulatory regimes. These principles are relevant to the outcomes we want to see across the sectors we regulate and for the people who use and rely on communications services.

Figure 1: High level summary of the Government's AI principles[9]

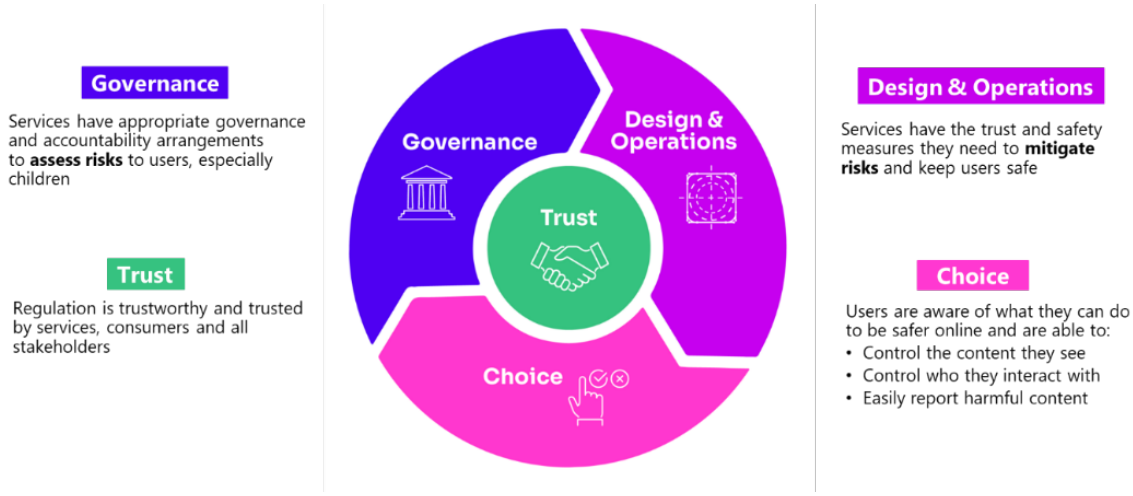
Principle	High level summary
Safety, security and robustness	AI systems should function in a robust, secure and safe way throughout the AI life cycle, and risks should be continually identified, assessed and managed.
Appropriate transparency and explainability	AI systems should be appropriately transparent and explainable.
Fairness	AI systems should not undermine the legal rights of individuals or organisations, discriminate unfairly against individuals or create unfair market outcomes. Actors involved in all stages of the AI life cycle should consider descriptions of fairness that are appropriate to a system's use, outcomes and the application of relevant law.
Accountability and governance	Governance measures should be put in place to ensure effective oversight of the supply and use of AI systems, with clear lines of accountability established across the AI life cycle.
Contestability and redress	Where appropriate, users, impacted third parties and actors in the AI life cycle should be able to contest an AI decision or outcome that is harmful or creates material risk of harm.

1.6 **Ofcom encourages industry stakeholders to adopt and embrace the AI principles where possible**. We recognise in our engagement with industry across telecoms, broadcasting and online safety that stakeholders are already considering how to make the most of the benefits of AI while addressing potential risks, and we look forward to our ongoing open dialogue in the context of the Government's AI principles.

[7] A deepfake replaces a person in an existing image of video with someone else's likeness with realistic results
[8] A pro-innovation approach to AI regulation: government response (February 2024)
[9] A pro-innovation approach to AI regulation: government response (February 2024)

1.7 **The OSA is an example of where similar principles have been actively considered by Parliament and underpin our legislative framework.** Many organisations regulated under the OSA are at the forefront of AI developments, and we can draw parallels between the key outcomes we would like to see and the AI principles. As seen in Figure 2, both the AI principles and our key outcomes for online safety emphasise the importance of appropriate **accountability** and **governance** in keeping users safe. We have also been clear that services must design and operate their services with **safety** in mind. Promoting **transparency** about services' safety measures and decision-making processes is important to ensuring that the online safety framework is trusted by services, consumers and stakeholders. In the interest of **fairness**, we want users to have the choice to control the content they see and who they interact with to keep them safe online. People should also have the choice to easily report harmful content when they see it, providing them with **contestability** and **redress** options.

Figure 2: Summary of Ofcom's key outcomes for online safety[10]



1.8 This document provides an update on Ofcom's strategic approach to AI through the following sections:

- Regulation of services that use AI technologies,
- Work to date to understand and tackle AI risks,
- Capability to address AI risks,
- Cooperating with others on AI issues, and
- Planned AI work.

[10] Ofcom's approach to implementing the Online Safety Act (October 2023)

2. Regulation of services that use AI technologies

2.1 **Ofcom invests in understanding the technologies used in our regulated sectors and their outcomes for consumers and the markets we regulate. We focus on the services that people use rather than the underlying technologies, including AI**. Ofcom is assessing the impact that AI may have in our sectors, and its implications for our ability to deliver on our regulatory outcomes.

2.2 We set out below examples of our regulatory powers and the related regulatory outcomes we have achieved, and will continue to achieve, taking into account the impact of AI.

- The **OSA** requires in-scope services to assess the risk of users encountering illegal or harmful content on their services, including risks associated with the deployment of AI-driven technology, for instance certain recommender systems (which suggest or recommend additional products to consumers). Services are then required to take proportionate measures to mitigate and manage the risks they identify. Priority illegal content, which the OSA requires services to take proportionate measures to prevent people from encountering, could include AI-generated child sexual abuse material. As part of work under the OSA, we could also recommend the use of AI-enabled safety technology within our Codes of Practice. An example of AI-enabled safety technology would be automated content moderation. This refers to the automatic analysis of text, images, and videos to detect and remove harmful content (e.g., hate speech, harassment, deepfakes and CSAM material). AI technology typically supports human moderators by filtering vast amounts of data quickly, allowing for more efficient and scalable moderation processes, ultimately creating safer online environments.
- Ofcom has set **'general conditions' for telecoms providers** as part of our duties under the Communications Act 2003.[11] AI can enhance the sophistication of scam calls and messages, and we have the power under our general conditions to instruct providers to block access to those numbers or services on the basis of fraud or misuse.
- Under the Telecommunications (Security) Act 2021 (TSA)[12], Ofcom has a duty to ensure that **telecoms providers take appropriate and proportionate measures to identify, reduce and prepare for security risks**. Providers can use AI to monitor for abnormal activities to detect and address issues more efficiently, identify potential vulnerabilities as well as conduct predictive risk analysis.
- Ofcom holds **competition and consumer powers** concurrently with the Competition and Markets Authority which could apply to digital services. AI systems could affect competition and consumer fairness outcomes in communications sectors, for example if they are used for personalised pricing, and we may have powers to investigate such matters.

[11] Communications Act 2003
[12] Telecommunications (Security) Act 2021

3. Our work to date to understand and tackle AI risks

3.1 **Ofcom has a wide programme of work in place to identify current and emerging AI risks and opportunities.** This section focuses on risks identified and highlights examples of our work to date to address them, and how our work links to the Government's AI principles. AI is used broadly in our sectors, and we have explored types of risk from the perspective of the consumer across sectoral boundaries. This enables us to mitigate cross-cutting risks more effectively and efficiently as we explore and tackle them in a more holistic way, leveraging our expertise as a converged regulator. We have set out key cross-cutting risks and our work to address them to date in Figure 3 which are:

a) Synthetic media[13],

b) Personalisation, and

c) Security and resilience.

3.2 To expand on one example, synthetic media can be used to generate harmful content that can reach UK citizens and consumers through online, broadcast and telecoms services. Although the type of synthetic media and the specific harms vary across our sectors, the overarching risk (harm to UK citizens and consumers) is the same, so we have grouped these together alongside examples of our work to date to address each cross-cutting risk.

3.3 **We have highlighted in Figure 3 below where we see links between the Government's AI principles and our work to date to mitigate AI risks**. We will continue to use the principles to assess AI risks that we identify and their impact on our regulatory outcomes, as well as, where appropriate, to inform any action we may take to mitigate them.

[13] Synthetic media is an umbrella term for video, image, text, or voice that has been generated in whole or in part by artificial intelligence algorithms

Figure 3: Areas of key risk & examples of Ofcom's work to date to address these risks

Key risks	Examples of our work to date to address risk
Synthetic media: AI tools that can be used to generate synthetic media can be used to create content that depicts child sexual abuse, acts of terrorism, and non-consensual pornography. They can also be used to generate more convincing mis- and disinformation, as well as more sophisticated and personalised fraud and scams. Such content can cause significant harm to individuals who are victims of it or who see it. The sophistication of these tools may mean that it is more difficult for users to distinguish between synthetic and real content.	• Published draft Illegal Harms Codes of Practice under the online safety regime, which include proposed measures in relation to **accountability** and **governance** to identify and manage risks, including risks posed by the sharing of illegal synthetic content.[14] • Launched a deep dive project to examine the merits of synthetic content detection methods that aim to improve the **transparency** of the synthetic nature of this content. • Commissioned and published research to understand adoption and attitudes towards GenAI.[15] • Published a media literacy discussion paper exploring the risks and opportunities created by GenAI, and how platforms, users and the media literacy sector could respond to these.[16] • Commissioned research and promoted best practice to support user groups most vulnerable to mis- and disinformation, which could be generated using AI.[17] • Published a Note to Broadcasters to clarify that they have **accountability** for their use of synthetic media generated by AI under the existing Broadcasting Code, including on **fairness.**[18] • Engaged with telecoms providers to understand and support their improvements to the **robustness** of scam message and calls identification and blocking, including by using AI, to protect citizens' **safety** and **security.**

[14] Consultation at a glance: our proposals and who they apply to (November 2023)
[15] Generative artificial intelligence poll: data tables (July 2023)
[16] Understanding Generative AI (February 2024)
[17] Ofcom supports organisations boosting online literacy skills in local communities (January 2023)
[18] Note to Broadcasters - Synthetic media (including deepfakes) (April 2023)

Key risks	Examples of our work to date to address risk
Personalisation: AI can be (and is) used by many of our regulated services to personalise the content served to UK users. This personalisation could, in the most serious of cases, lead to the amplification of illegal and harmful content online. It could also affect the discoverability of UK and public service content, including news content, exacerbating the existing trend of echo chambers. Some of the services we regulate can also apply AI to large customer datasets to personalise the price of services offered to UK consumers, based on their individual characteristics. This potentially could lead to price discrimination. A lack of transparency around AI and personalisation could affect the ability of UK consumers to make informed choices about the content they consume and the services they use.	• Published draft Illegal Harms Codes of Practice under the online safety regime, which include proposed measures recommending that certain services collect **safety** metrics when testing recommender systems (which may include AI-driven systems), to improve online **safety.**[19] • Published a third-party paper exploring methods that online platforms can take to test and evaluate AI driven recommender systems to understand their impact on online **safety.**[20] • Published our view on the role online intermediaries (e.g., search engines, news aggregators, social media) play in the consumption of news content, including their lack of **transparency,** which we will build on as we engage with the Government on the draft Media Bill and develop our own proposals to safeguard trust in news in our upcoming review of Public Service Media.[21] • Published a discussion paper on personalised pricing, which highlighted the importance of giving some **transparency** around the process to arrive at price and enabling consumers to compare prices effectively.[22]
Security and resilience: More advanced forms of AI, like GenAI, could be used to develop more virulent malware, identify vulnerabilities in networks, and/or provide instructions on how to breach network security. Poorly developed GenAI models could also contribute to the risk of system outages. For example, if source code is inefficient in its use of energy or bandwidth, or widespread use of the code by applications leads to an overall resource outage.	• Tracked developments in how GenAI could be used to develop malicious tools that threaten network **security.** • Engaged with regulated services covered under the TSA to understand how they are integrating GenAI into their systems, including how they are considering **robustness** and **security** both in their own systems and across their vendor supply chains. • Engaged with standards bodies (e.g., the European Telecommunications Standards Institute and the International Organisation for Standardisation) which are developing standards, including on **robustness** and **security** for language models that underpin GenAI tools. This might have relevance across Ofcom's remit.

3.4 **As some companies regulated under the OSA are at the forefront of AI developments, we have carried out additional work in this area.** In addition to the cross-cutting work set out

[19] Consultation at a glance: our proposals and who they apply to (November 2023)
[20] Pattern Analytics Intelligence Report (July 2023)
[21] Discussion document: Media plurality and online news (November 2022)
[22] Personalised pricing for communications: Making data work for consumers (August 2020)

in Figure 3, we are carrying out further work specific to online safety which also aligns well with the Government's AI principles. Examples include:

a) Undertaking internal research on the technical challenges of assuring a user's age using AI-driven technology. When considering if a service has complied with its relevant duties, we will consider **transparency** and **accountability**.

b) Ongoing research into the merits of red teaming[23] to detect vulnerabilities in AI models and tools, which could be used to help ensure their **robustness** and **security**.

c) Ongoing research into the merits of synthetic media tools, which would provide greater **transparency** over the synthetic nature of any content. We will also keep promoting best practice support to user groups who are most vulnerable to mis- and disinformation that includes synthetic media, giving them tools to improve their online **safety**.

3.5 **We will continue to carry out horizon scanning work across our sectors to identify potential risks and benefits that AI could have for UK citizens and consumers.** Through our horizon scanning work (including joint work with other regulators via the Digital Regulation Cooperation Forum (DRCF[24])), we will continue to identify the risks and benefits that AI could have for UK citizens and consumers. This will include considering how AI could impact our existing priority outcomes, and whether it means we should consider new priority outcomes. This work will also take into account the Government's AI Principles. Ofcom will collaborate closely with the Central AI Risk Function housed within the Department for Science, Innovation and Technology (DSIT) to identify, measure and monitor existing and emerging AI risks.

[23] Red teaming involves structured, creative and critical thinking techniques to challenge existing thinking to help develop a better-informed decision or more robust product

[24] Members include the Competition and Markets Authority (CMA), the Financial Conduct Authority (FCA), the Information Commissioner's Office (ICO) and Ofcom

4. Our capability to address AI risks

4.1 **Ofcom has always needed technical knowledge and expertise to exercise our functions and perform our duties effectively.** This supports our robust assessment of the opportunities and risks arising from new forms of technology. We have over 100 technology experts (with approximately 60 AI experts) in our data and technology teams, including some with direct experience of developing AI tools (e.g. computer vision for age estimation technologies, speech moderation app which uses AI to check if speech is harmful to the 9 protected characteristics and an application to create invisible watermarks on images) who are supporting our understanding of the impacts and risks of AI on our sectors and stakeholders. We continually assess and review our capabilities to ensure we have the expertise we need.

4.2 **We are building strategic partnerships with academic institutions,** such as the National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online (REPHRAIN) to share knowledge. This includes us sharing the risks and challenges from AI that our in-house experts have identified through carrying out or commissioning their own technical research. To date this research has been carried out on areas including hashing (converting data into a fixed-length string of letters and numbers which can be used for applications such as cybersecurity and data privacy)[25] and automated content classifiers (often using machine learning to automatically classify what type of genre certain content is) for live streaming.[26]

4.3 **We are developing our data skills across Ofcom.** Through our data strategy, we are developing a data culture and data literacy programme which will increase knowledge and understanding of AI across our organisation. We are supporting colleagues to understand the opportunities and risks that AI technology presents in a variety of ways, including through targeted learning and development. We are also looking into how we might use AI to improve our work and efficiency.

[25] Overview of Perceptual Hashing Technology (November 2022)
[26] Automated Content Classification (ACC) Systems (January 2023)

5. Cooperating with others on AI issues

5.1 **Ofcom regularly engages with other domestic and international organisations, to collaborate on AI-related issues, and will continue to do so.** For example:

- **Ofcom is a member of the DRCF.** Through the DRCF we have been collaborating with other UK regulators on algorithmic processing, audits and AI governance, as well as taking a new focus on GenAI. We will continue working together on AI and algorithms, for example by examining the key tenets of fairness in algorithmic decision-making and investigating the market of third-party algorithmic auditing firms. The DRCF is preparing to launch the AI and Digital Hub to support digital innovators.[27] The Hub will enable innovators to direct their complex, cross-regulatory questions through a single point of access and receive tailored support. The aim of the service is to increase innovators' confidence to launch innovative digital and AI products in a safe way and reduce the time that it takes for innovators to bring products and services to market. All firms will be able to benefit from the support that we provide through an accompanying case study archive. The DRCF will set out more information about our plans for cooperation in its upcoming workplan.
- **Ofcom is a founding member and current Chair of the Global Online Safety Regulators Network (GOSRN)**, a growing network of regulators with responsibility for online safety which to date includes regulators from Australia, Fiji, Ireland, South Korea, South Africa and France**.** Through the GOSRN we are sharing our experiences and learnings about AI-related issues to better understand the risks and opportunities that AI technologies pose to our work as online safety regulators. The focus will initially be on technical solutions to protect children online and how to manage the safety challenges of GenAI.
- **Ofcom is also a member of the European Platform of Regulatory Authorities (EPRA),** a network of over 50 European (EU+) audiovisual regulators. Through EPRA's AI Roundtable, we are exchanging experiences with EPRA members on the use of AI tools in broadcasting regulation, and on the impact that AI technologies are having on the broadcasting sector.
- **We are proactively following policy debates globally on AI, across the sectors we regulate.** This includes engaging directly with civil society, academics, and policymakers around the world to understand the uses and impact of AI. This engagement has seen us contribute to the development of Council of Europe guidelines, published in December 2023, on the responsible use of AI systems in journalism, and we have a seat on the Forum for Information and Democracy's AI Research Assessment Panel which will make policy recommendations at the end of 2024. Ofcom is also following discussions on AI standards in standards development organisations including at the International Telecommunication Union (ITU), where Ofcom represents the UK.

[27] The DRCF AI and Digital Hub – Supporting digital innovators (September 2023)

- **Ofcom regularly engages with the Government on AI, both bilaterally and through the DRCF, including on the set up of the Government's Central AI Risk Function.** Ofcom has updated the Government on the impact of AI in our sectors and the implications for our work during the development of the Government's AI regulatory framework. Ofcom has also engaged with the Government, including as part of the DRCF, on how regulators might engage with the Government's Central AI Risk Function. As the Government takes forward its plans, we will continue to examine risks posed by AI and to analyse and review potential gaps in existing regulatory powers and remits and coordinate with the Government on these matters where appropriate. We are also engaging with the Scottish Government and monitoring the implementation of its AI Strategy with our Chief Data Officer sitting on the leadership Group of the Scottish AI Alliance, the body responsible for delivering the strategy.

6. Our planned AI work

6.1 **Ofcom's planned AI work will ensure that we continue to identify and respond to AI related risks across our remit.** This will include continuing to execute and evolve many of the key activities that we have set out in this document, as well as starting new work across our different policy areas. Examples of this work are set out in the Annex of this document.

A1. Planned AI work for 2024/25

Ofcom's Plan of Work 2024/25 sets out the planned work that we will carry out over the next 12 months. As AI has relevance across our remit, many of these projects will undertake work to consider AI's impacts, even if this is not explicitly referenced. This Annex provides examples of the AI work that we will carry out in each of our policy areas as well as work that cuts across our policy areas.

Policy area	Work we will do in 2024/25
Online safety	• Draw up and consult on Codes of Practice measures as appropriate to help regulated services tackle risks, to protect users from illegal and harmful content. • Research the merits of red teaming to detect vulnerabilities in AI models and tools, the merits of synthetic media detection tools, and the merits of automated content classifiers. • Research the merits of using GenAI for content moderation, as well as potential methods for preventing children from encountering GenAI pornographic content. • Consult on guidance relating to Ofcom's information gathering powers, including powers which may be used to gather information about algorithms/functionalities, where relevant.
Broadcasting	• Issue guidance as needed and appropriate to broadcasters to clarify their accountabilities in relation to AI. • Engage with broadcasters to understand how GenAI may reduce their production costs and the implications stemming from this. • Consider the implications of AI driven recommender systems for media plurality and sustainability, and the discoverability of public service media content. • Understand whether developments in AI could accelerate the decline in viewing of broadcasting content. • Consider what the implications of AI broadly mean for public service media as part of our Public Service Media Review.

Policy area	Work we will do in 2024/25
Telecoms	• Monitor AI related fraud and scams risks by engaging with industry. • Monitor AI related cyber security risks across the vendor supply chain by collecting intelligence through engagement with industry. • Monitor how AI can be used to counter cyber security risks across the vendor supply chain through engagement with industry. • Flag any concerns around negative impacts of AI on telecoms security to the appropriate entities (Government, regulated services, and law enforcement). • Use our regulatory powers to investigate security compromise reports from services in scope of the TSA and identify if these have been facilitated by AI risks. • Monitor and engage with standards bodies domestically and internationally which are developing AI standards. • Monitor AI market developments to understand their impact on telecoms markets, including competition.
Crosscutting	• Monitor and engage with AI developments internationally, including the EU's AI Act. • Engage in domestic and international regulatory forums, including the DRCF, GOSRN and EPRA, on AI issues that cross regulatory remits. • Horizon scan to identify emerging and longer-term AI developments that could have implications for citizens and consumers, regulated services and regulated sectors. • Engage with the Government, including through its Central AI Risk Function. • Build our AI capabilities by upskilling our talent and exploring how we can leverage AI across our operations.