Ofcom's strategic approach to AI, 2026/27

Enabling safe and secure AI adoption

Welsh version available

Published 4 June 2026
For more information on this publication, please visit ofcom.org.uk.

Contents

Section

Annex

1. Introduction

1.1 **AI continues to transform our industries and our everyday lives.** As its capabilities progress at an extraordinary pace, we are seeing new applications and opportunities for innovation within our sectors. These exciting developments, however, are also accompanied by new and evolving risks.

1.2 **Over the past year, we have seen AI adoption increase among consumers and our sectors.** Ofcom's research suggests that over half of adults (54%) report using AI tools such as ChatGPT, Copilot, or Gemini[1] – a rapid increase compared to the 31% of adults who said the same in 2024.[2] Meanwhile, our sectors are now routinely deploying generative AI (GenAI), from BBC Sounds' trial use of AI for personalised streams of audio content[3] to Google's AI-generated search result overviews. Interest in emerging technologies such as agentic AI,[4] is also growing, with our research identifying current and potential future use cases including autonomous content moderation, postal delivery route optimisation and telecommunications network maintenance. Further details can be found in Annex 2.

1.3 **As AI capabilities and adoption increase, so too does the creation and amplification of harms.** The AI Security Institute's (AISI) evaluation of AI cyber capabilities found that models were capable of completing expert-level tasks (typically requiring 10+ years of experience) in 2025, up from apprentice-level (less than a year of experience) in 2023. With these advancements, cyberthreats may increase in scale and speed as models become better at exploiting vulnerabilities, as highlighted in AISI's assessment of Claude Mythos. In online services, over one in five (22%) internet users now report encountering fake or deceptive images or videos online.[5] Furthermore, we're seeing increasing misuse of chatbots and the development of nudification apps to create non-consensual sexual deepfakes and deepfake fraud content.

1.4 **This document sets out our approach to AI in response to the Government's request for regulators to demonstrate how they are supporting the UK's growth agenda,** as set out in the AI Opportunities Action Plan. It will explain how we apply our broadly technology-neutral, outcomes-based regulatory principles to AI and demonstrate our role in enabling safe and secure AI adoption.

Our Approach

1.5 **As the converged regulator for the communications services that consumers and businesses across the UK use and rely on each day, our mission is to make communications work for everyone.** Our pro-innovation approach means we welcome AI adoption for its potential to deliver positive outcomes for our sectors, while remaining committed to safety, security and mitigating the risks that technology might create or

[1] Adults' Media Use and Attitudes 2026 Report
[2] Adults' Media Use and Attitudes 2025
[3] Media Nations 2025 - UK Report
[4] Agentic AI refers to artificial intelligence systems that take goal-directed actions autonomously – they plan, make decisions, and execute tasks without constant human input.
[5] Online Nations Report 2025

amplify. Where markets are unable to mitigate these risks, to the extent that we can, we will apply our existing powers to prevent harm.

1.6 **Against a rapidly shifting landscape, we have acted decisively to address emerging risks, support our sectors, and develop our knowledge and capabilities.** We coordinated with AISI and the National Cyber Security Centre (NCSC) to update stakeholders on frontier AI's cybersecurity implications after Anthropic's preview of Claude Mythos caused widespread concern, and we were the first national regulator to launch a formal investigation into X's Grok chatbot.

1.7 **In parallel, we are taking proactive steps to enable safe and secure AI adoption across the communications sector.** In our Deepfake defences research, we set out technology-led mitigation techniques to help organisations safeguard against deepfakes, while demonstrating how AI itself can positively reduce harm created by nefarious actors. We are also directly engaging entrepreneurs, startups, and SMEs to gain a clearer view of where regulatory uncertainty might hinder AI adoption, so we can respond accordingly. Alongside this, our research on the impact of AI on telecoms customer experience will help us assess whether existing rules provide sufficient consumer protection to support safer AI adoption.

1.8 **We are additionally engaging with the UK Government to prepare for increased regulatory responsibilities relevant to AI.** We will support the Government's work to introduce secondary legislation relevant to grant Ofcom powers to protect users including by engaging with the Government to ensure the workability of provisions following the Crime and Policing Act and the Schools and Children's Wellbeing Act. We are also preparing for new responsibilities regarding data centres – a critical part of AI infrastructure – as part of the Cyber Security and Resilience Bill, which is currently before Parliament. Finally, we will continue to use our powers under the Communications Act 2003 (as amended by the Telecommunications (Security) Act 2021 (TSA)) to address security and resilience risks arising from AI in telecoms networks.

1.9 **Alongside supporting businesses and consumers, we have been investing in our own internal AI capabilities and piloting responsible AI adoption across many elements of our work.** We have strengthened our AI governance framework, improved the ways in which we train and upskill colleagues across the organisation and are experimenting with how AI might support our research and policymaking functions in ethical and accountable ways.

1.10 **The update to our *Strategic Approach to AI* that follows explains this work in more detail and is structured around four pillars:**

- *'Applying our regulatory principles to AI'* goes into further detail about how we understand our relationship with AI given our status as a technology-neutral, converged regulator
- *'Our work to enable safe and secure AI adoption'* showcases our case studies to demonstrate where we are supporting AI innovation and managing AI risk across our sectors
- *'Our approach to AI in practice'* explains more about the research we have conducted, details how collaboration underpins everything we do, and sets out how we are approaching AI use internally
- *'Our planned work'*, included as an annex, looks to the future and highlights our awareness of how our work in this area must continue to evolve.

2. Applying our regulatory principles to AI

2.1 **Achieving the best outcomes for citizens and consumers will always be central to our mission.** We believe good regulation can foster innovation, encourage investment and support economic growth, as well as promote safety and protect consumers against harm. AI can also help us achieve our aims – from enhancing cybersecurity vulnerability testing to autonomously moderating content online – and is already reshaping how industry can manage risk.

2.2 **To that end, we apply our regulatory principles consistently to AI and other cutting-edge technologies, as follows:**

When we regulate

- **We operate with a bias against intervention, but with a willingness to intervene promptly and effectively where required.** We want to create the best conditions to help our sectors take advantage of the opportunities AI has to offer, without imposing unnecessary burden or barriers. However, where AI-enabled harms arise, we will use our powers to take swift and targeted action to protect our citizens and consumers.

- **We intervene where there is a specific statutory duty to work towards a goal that markets alone cannot achieve.** We take our responsibility to protect UK citizens and consumers with the utmost seriousness, especially the most vulnerable or those most likely to face AI-enabled harm. Where markets are unable to mitigate these risks, to the extent that we can, we will use our existing powers to prevent harm.

How we regulate:

- **We always seek the least intrusive regulatory methods of achieving our objectives.** Our regulation is broadly technology-neutral and outcomes-focused. This means we focus on regulating outcomes for consumers and citizens, not on whether particular technologies should or should not be used to deliver them. This empowers our regulated sectors to deploy AI without seeking our approval provided they are confident they can do so responsibly.

- **We strive to ensure that interventions are evidence-based, proportionate, consistent, accountable and transparent in both deliberation and outcome.** Central to our approach is avoiding unnecessary and burdensome regulation on our sectors. Instead, we assess emerging AI-enabled risks on an ongoing basis, remaining mindful of context, the macroenvironment, and existing laws and legislation.

- **We regulate with a clearly articulated and publicly reviewed annual plan, with stated objectives.** Regulatory uncertainty can be a barrier to adoption, so we seek to provide clarity about how regulation is being applied, helping our sectors to confidently innovate with AI. This paper, among other documents, helps provide this clarity.

How we support regulation:

- **Ofcom will research markets constantly and will aim to remain at the forefront of technological understanding**. Drawing on a robust evidence base helps us regulate AI

with agility and ensure our regulation is fit-for-purpose as technologies and markets evolve.

- **Ofcom will aim to consult widely with all relevant stakeholders and assess the impact of regulatory action before imposing regulation on a market.** We engage external experts, including other regulators, to strengthen our understanding of AI and share best practices to inform our decision-making.

3. Our work to enable safe and secure AI adoption

3.1 **We have a role as an enabler to support AI innovation in our sectors.** In our upcoming work – as we have done in the last 12 months – we will consider how we can further support AI innovation and adoption in our sectors.

3.2 **We have an important role to play in promoting consumer safety and building their trust in new technologies.** AI has impacted consumer safety across our sectors, creating and enhancing a number of risks. These risks include exposure to harmful deepfakes which can cause significant distress to people, as well as enable more sophisticated fraud and scams and the spread of mis/disinformation. AI-generated content can also cause harm even when it is not used maliciously, as it can create unintentional inaccuracies which can reduce trust in content, especially news. AI can also lead to increased security risks as it allows cyberattacks to be crafted quickly and cheaply – this can then lead to data leaks or system outages, both of which can harm consumers. To help keep consumers safe from these risks, it's important they have the right level of trust in AI – too much trust can make people more likely to believe harmful and misleading outputs, and not enough trust could make people reluctant to use certain services and feel isolated. We aim to mitigate the risks presented by AI through our policy and research work.

3.3 **We anticipate that AI adoption will advance at different speeds across and within our sectors.** This means that some areas of the AI landscape are similar to last year, and we consequently have ongoing pieces of work to explore how we can enable the same benefits and protect citizens and consumers from the same harms that we have previously discussed.

3.4 **We have therefore decided to focus our update on specific examples of how we are enabling safe and secure AI adoption in each of our sectors**. The rest of this section details these examples as case studies. A more comprehensive summary of our planned AI work for 2026/27 can be found in Annex 1.

Case studies on how we enable safe and secure AI adoption across our sectors

We're strengthening the foundation for adoption...

3.5 Creating the right foundation for AI adoption is crucial to help industry unlock the benefits of AI and support innovation. The following case studies detail how we are **cleaning up our data to make it more useful for our stakeholders**, and how we are **directly engaging with innovators to provide regulatory clarity** so they can safely and securely use AI:

Case study 1: Building a data lake for spectrum licence information and online safety data

What we are doing

Ofcom currently makes available a range of data through online portals and open data files. We are presently building a data lake[6] to consolidate and store a wider range of data, structuring the underlying data sets to make them more accessible to industry and the public. This year we plan to make available several types of spectrum licence information, including Fixed Links, Business Radio, and Shared Access. We are also describing and cataloguing reusable online safety data sets that can be used for machine learning and agentic queries, to be stored within this data lake.

The difference it will make

Establishing and maintaining data context and quality is essential for successful AI model use which requires detailed modelling and labelling, and is often a complex and ongoing process. To build our data lake, we are cleaning up our existing data to make it more useful for AI. For instance, we have aligned internally on definitions of different types of data, using consistent terminology and clarifying data entries. Improving the quality of our data helps us to build on a solid foundation to make data more accessible and useable, and help enable AI adoption in our sectors.

Case study 2: Innovation support

What we are doing

We have launched a programme of engagement with innovators across our remit to improve our support for UK innovation. We've engaged with over 60 entrepreneurs, startups, SMEs and industry stakeholders, many of whom leverage AI to enable the services they offer but also use AI tools to understand and navigate regulation.

As part of our engagement, we've explored the experience of these companies innovating in the sectors we regulate, the challenges when engaging with our regulatory processes, and how Ofcom can provide further support for innovators.

We will further build and strengthen our engagement with the innovation community and invest in select activities where we believe we can best support innovation.

The difference it will make

Stakeholders tell us that regulatory uncertainty is a barrier to AI adoption: our work aims to boost industry understanding of our regulatory approach, which can give innovators greater confidence around regulatory compliance – ultimately enhancing opportunities for new technologies while ensuring the safety of consumers. Alongside our fellow Digital Regulation Cooperation Forum (DRCF) members, we are considering a suite of options – including investigating GenAI solutions – as part of a wider effort to address regulatory barriers in the UK.

We're understanding and mitigating online harms…

3.6 Deepening our understanding of AI-powered tools is also important for Ofcom as the regulator for online safety as many of the services we regulate make use of AI features –

[6] A data lake is a central location that holds a large amount of data both in its raw (original) form, and in further layers of cleaned-up and processed forms.

ranging from age assurance technologies to GenAI chatbots. The following case studies explore our work to **understand and mitigate the potential online harms these AI features could cause, to maintain user safety**:

Case study 3: Deepfake Defences

What we are doing

We have been investigating the causes and consequences of a rise in the number of harmful deepfakes online. We first published a discussion paper, Deepfake Defences, that examined the nature of deepfakes, setting out a typology covering those that are intended to demean, defraud and disinform. The paper set out a range of mitigation options that could be deployed at different points in the AI lifecycle, from AI developers applying output filters to their models, to search engine providers taking action to downrank websites hosting deepfakes. Our second discussion paper, The Attribution Toolkit, delved into the merits of so-called 'attribution' measures, including AI labels and metadata schemes. The paper includes the findings of our in-house technical experiment of common watermarking schemes, which revealed the extent to which watermarks could be removed from images.

The difference it will make

Deepfakes are a growing problem. Over 1 in 5 (22%) of internet users now report encountering fake or deceptive images or videos online.[7] Our research findings enable Ofcom to develop more robust policy options for countering their spread. For example, drawing on these insights, we have been able to assess the merits of different techniques for preventing the creation of deepfake fraudulent adverts – something that has directly informed the development of our draft Fraudulent Advertising Code of Practice. This Code will be published as part of a wider online safety policy consultation in the summer.

The discussion papers are also a source of intelligence for actors in the wider online safety community as they seek to tackle deepfakes. Our Deepfake Defences paper lists a dozen distinct and promising mitigation methods that are available to deploy today. Our Attribution Toolkit, meanwhile, identifies where some of these methods could be further improved (e.g. making watermarks more resistant to tampering). We hope that AI developers and safety technology firms bear our findings in mind as they continue to iterate their deepfake safeguards.

Case study 4: Trust and AI chatbots

What we are doing

Recent Ofcom analysis on AI and media literacy has highlighted that users, companies and institutions often have a tendency to anthropomorphise AI chatbots – that is, to describe or treat these systems as though they have humanlike qualities.

The ways in which language and presentation influence people's trust in one another, trust in information, and trust in automation is under-researched yet fundamental to our understanding of GenAI and how it is used. Our 'Trust and AI chatbots' research, will help to build on this scarce research base, by focusing directly on how language shapes public use, understanding and trust in AI and what it means for media literacy.

The difference it will make

Little is currently known about how people perceive, talk about, and place trust in AI chatbots, and what this means for the media literacy skills they use when engaging with them.

[7] Online Nations Report 2025

By examining usage, attitudes, and the role of anthropomorphisation, we will gain insights that can support best practice in product design and improve understanding of where and how harms may develop.

We're using our understanding of AI to inform our policy development...

3.7 We have also been working across our sectors to **understand the potential impacts, both positive and negative, of AI on consumers and industry**. The following examples detail our work with industry across telecoms and broadcasting to **support our policy development** in the world of AI:

Case study 5: The impact of AI on the experience of telecoms customers

What we are doing

Telecoms companies and their customers have increasingly adopted AI tools in recent years for a range of applications, taking advantage of rapid innovation in the underlying technologies. We want to understand how residential and business customers, telecoms companies and third-party applications in the telecoms value chain are currently using AI tools and technologies. We are also exploring the potential future evolution of the use of customer-facing AI in telecoms and how these trends may change customers' experience of engaging with telecoms markets.

We are conducting research into customers' awareness of and ability to use AI tools, exploring developments in international telecoms markets and other sectors of the UK economy. We plan to publish our findings in the second half of 2026.

The difference it will make

Within the context of rapid AI development, it is important that we understand the impact that AI tools and technologies could have on telecoms markets and the experience of telecoms customers.

As part of this work, we are also considering if any changes to our rules are required to protect customers from potential harms. For example, we might consider whether the specific protections we have in place for consumers in vulnerable situations are adequate, whether adoption of AI might heighten the risk that people and businesses become victims of fraud and whether protections might be needed for customers who do not feel comfortable using AI tools.

Case study 6: AI use in the broadcasting sector

What we are doing

We have undertaken a research exercise, including engaging directly with entrepreneurs, traditional studios, and AI-native production houses, to build an evidence-based view of how AI is being used in UK broadcast, production, and the wider media sector. Our findings have clarified where AI is (and is not yet) being used across the content creation and GenAI value chains, and what is holding adoption back. We have also gained insights on synthetic media capabilities and the risks these can pose to audiences and broadcast services.

The difference it will make

AI can provide a lot of potential benefits to the creative industry, including greater efficiency, new creative workflows, and increased revenue opportunities. However, our work has found that there are practical barriers to unlocking these benefits such as copyright uncertainty, skills

and education gaps, reputational risk and current technical limitations. We are building a shared evidence base for industry to better establish best practices, increase know-how, facilitate innovation and eventually potentially establish standards. We are also identifying where convening industry or encouraging voluntary coordination could reduce friction for responsible AI deployment.

AI can also increase risks in broadcasting. Our work highlights risks from synthetic media for audiences and services, including misuse, reduced trust in content (especially news), and compliance and safeguarding challenges in live contexts.

Our ongoing research and engagement will inform our policy development, our discussions on emerging risks and opportunities with broadcasters, and wider considerations on how the sector will develop in the interests of audiences.

We're building trust in infrastructure...

3.8 Our stakeholders play an important role in **providing the necessary infrastructure to enable the deployment of AI**. We have **duties to ensure that these networks remain safe and secure** – the case studies below provide more detail on our work in this area:

Case study 7: AI and cyber security

What we are doing

We are seeking input from operators regulated under the Communications Act 2003 (as amended by the Telecommunications (Security) Act 2021 (TSA)) and the Network and Information Systems (NIS) Regulations 2018 to understand how AI is currently being used in cybersecurity and whether regulatory requirements may present unintended barriers to adoption. This comes at a time of immense upheaval in the cybersecurity world with the arrival of AI models like Mythos that could make mounting attacks on networks easier and faster to achieve than ever. We will be engaging with a broad range of partners for this work. Our initial focus is on industry, specifically with companies regulated by the TSA and NIS.

Our work builds on the DRCF's horizon-scanning event on the Future of Cybersecurity and Emerging Technologies which explored with industry and others both how AI can be harnessed to tackle cybersecurity threats, and strategies for the cybersecurity community to understand and mitigate risks posed by AI, such as those posed by the latest large language models.

The difference it will make

In regulated cybersecurity environments, operators must balance safe and secure innovation against regulatory risk. Levels of trust and assurance in AI, which are important given the regulatory requirement for strong oversight and understanding of security control, are therefore likely to affect both the pace and extent of its adoption across the telecoms and digital infrastructure sectors. Our monitoring suggests that AI trust and assurance are improving, as evidenced by decreased hallucinations and increased verifiability of sources in reasoning models, but that issues persist.

This work aims to bolster the security of telecommunications networks and information systems by providing regulatory clarity and confidence to industry. In turn, this could ensure that as far as current technology allows, unintended or perceived regulatory barriers to adoption are addressed.

We envisage carrying out related work in the vendor and third-party assurance space, and we will continue to engage with DSIT – in particular, AISI – and other partners. Our insights from all

of our work on cyber security and AI will feed into our policy work and could support government decision-making, helping ensure that regulation and its implementation do not inadvertently hamper the use of effective defensive technologies.

Case study 8: 'AI for Networks' and 'Networks for AI'

What we are doing

Our research on 'AI for Networks' explores how AI is being applied, or could be applied, by telecoms providers to support network management and optimisation, including in areas such as fault prediction, and performance management. We are investigating how AI can improve network efficiency in terms of resilience, reliability, and service quality, while considering emerging areas around transparency, explainability, and accountability in network operations.

Alongside this, our research on 'Networks for AI' focuses on investigating how networks could reliably support AI applications and AI-enabled services at scale. This includes understanding requirements relating to connectivity, capacity, performance, and coverage, and understanding where the market is likely to deliver through existing network assets, and where constraints may remain.

The difference it will make

The telecoms sector could benefit significantly from AI, as applications utilising the technology begin to improve network efficiency and the operation and maintenance of telecoms networks.

Our work on 'AI for Networks' can help inform our policy development on network resilience for telecoms providers, which may lead to appropriate expectations to be included in future guidance, helping our sectors to deploy AI safely and securely.

In parallel, our work on 'Networks for AI' considers how telecoms networks are evolving to support the growing use of AI across the wider economy.

4. Ofcom's approach to AI in practice

4.1 **Our approach to understanding and using AI in practice helps underpin our regulatory thinking.** Through our research work and technical expertise, we have a deep understanding of how the technology is currently used in our sectors, and how it could be used in future. We also regularly collaborate with other organisations both abroad and at home to keep up to date on wider AI developments and inform our work. Finally, we are further developing our own AI use, including experimenting with how we can use AI to support our research, policymaking functions and internal processes to help make them more efficient.

Our AI research and understanding

4.2 **As AI continues to transform our sectors, we're ensuring we have the understanding, expertise and capabilities to respond to technological and market changes, enabling innovation and safeguarding users**.

4.3 **We are building on our AI knowledge through our market research.** Earlier this year, we carried out research on agentic AI use cases[8] to understand the state of play and help build a foundation of knowledge of how to best support our sectors. Our findings suggest that although most use cases in our sectors are currently at a prototype stage, agentic AI has the potential to amplify the existing impacts of AI – both positive and negative. These positive and negative impacts are often linked, with the benefits also coming with trade-offs; for example, agentic AI could bring greater personalisation at the cost of reduced exposure to a diverse range of viewpoints. We will consider these findings as we prepare for our sectors to use agentic AI more widely.

4.4 **We're also conducting our own technical research.** Ofcom remains a technology- informed organisation – it is important that we understand details of the tools our sectors are using in practice. Many of our technical experts work across online safety, including in our Online Safety Technology Lab (OST Lab), and on telecoms and digital infrastructure – more detail is set out below.

- The OST Lab is a hybrid physical and digital environment where Ofcom can undertake in-depth testing and evaluation of existing and emerging approaches to online safety. This lab allows for the examination of specific technical solutions, such as those in watermarking and content moderation. With this in-house capability, Ofcom's technical experts can quickly initiate experiments and projects to address technology and policy questions, producing our own research to support evidence-based policy making and ensuring their knowledge keeps up with the rapid pace of change in the technology industry.
- We draw on our technical expertise in telecoms networks and infrastructure to understand how AI is changing both network operations and network requirements. We complement this with horizon scanning and targeted technical engagement across key parts of the connectivity value chain. We also draw on our technical expertise to

[8] A more detailed summary of our research can be found in Annex 2.

support related policy work in broadcasting and media as we anticipate the use of AI in the personalisation of content navigation experiences and the development of enhanced assistive technologies (such as subtitling, audio description, dialogue enhancement and navigation).
- In network security, we use our technical expertise to consider the opportunities and the challenges that AI brings to the cyber realm – from the immediate technological impacts on security operations to the broader evolutions they will bring to security frameworks, policy and governance.

4.5 **We attract and retain technical experts by offering the opportunity to work hands-on with emerging technologies on complex, real-world regulatory challenges**. Our specialists work alongside policy, legal and other experts, with scope to deepen technical expertise, influence regulatory outcomes, and build sustainable careers within a public-interest organisation.

4.6 **We will continue to engage with industry and external experts to maintain our understanding of how our sectors are using and plan to use AI.** We encourage our stakeholders and wider industry to maintain an open and up-to-date dialogue with us to help us work together to meet our aim to enable safe and secure AI adoption across our regulated sectors.

4.7 **We're closely monitoring developments in the wider AI landscape to better understand the impacts these would have on consumers and businesses.** As AI adoption accelerates, reliance on a small number of global AI providers is increasing. We actively draw on industry analysis and insights from our stakeholders to assess how these market dynamics affect the sectors we regulate, including impacts on competition and financial resilience of relevant stakeholders.

4.8 **We're preparing for future developments through horizon-scanning, taking a holistic approach looking across our sectors.** We have investigated how AI will impact our sectors across the entire AI tech value chain to understand the opportunities and challenges emerging. Through this work, we have explored cross-cutting themes of security, resilience, and trust which arise throughout the chain, providing a solid baseline to better understand AI developments at a global level.

Our collaboration on AI

4.9 **Ofcom regularly collaborates with other domestic and international organisations on AI-related topics, which sit across regulatory and state boundaries, for the benefit of industry and consumers.** For example:

- **Ofcom engages with the Government on AI across a broad range of issues.** We welcome the potential that AI has to catalyse economic growth across the UK and are focused upon supporting this agenda across the sectors we regulate. This includes publishing and making large datasets available to industry, supporting the training and development of AI models and helping unlock benefits for the UK communications sector more quickly. We also continue to work closely with partners from AISI to support knowledge exchange around shared interests including AI safety.
- **Ofcom is a founding member of the DRCF.** As set out in the DRCF 2026/27 Work Plan, there will be a renewed focus upon close collaboration around AI related issues and opportunities in the next twelve months. More details of this work, and our DRCF work on AI over the last year, are set out below:

- During 2025/26, the DRCF focused the work of its thematic hub on agentic AI – bringing together representatives from member regulators, industry and the research community to explore key questions and issues around this specific topic which was published at the end of March. It also convened the second Responsible AI Forum, bringing together experts from industry, government and academia for deep, constructive conversations about the risks and opportunities of AI for the UK.
- In addition to hosting the third Responsible AI Forum, DRCF will undertake research into how consumers will engage and respond to the growing deployment of AI in everyday life and the future of robotics and physical AI.
- The DRCF provides us with a shared space to test and build new ways of supporting business and removing barriers to innovation. The aim is to support businesses to bring AI and digital products and services to market responsibly, faster and with greater confidence.
- As part of its work to promote capacity building, the DRCF will support ongoing work to explore advanced regulatory technologies and the development of specialist skills and capabilities across the four member regulators.

- **We will work with the new Scottish Government on its commitments to take forward the interventions in Scotland's Artificial Intelligence Strategy 2026-2031,** including on the place of regulation, for example as part of the Data Centres and Infrastructure layer of the Scottish Government's 'AI Stack'.
- **We are working to bring Ofcom's expertise to international discussions on the impact of AI in our sectors.** This includes contributing to the Organisation for Security and Co-operation in Europe's (OSCE) recent report on Safeguarding Media Freedom in the Age of Big Tech Platforms and AI. We have also helped develop Council of Europe guidelines on the responsible use of AI systems in journalism and acted as an observer to the Observatory for Information and Democracy's AI Research Assessment Panel. And in the Global Online Safety Regulators' Network, we have recently joined workshops and policy deep dives on AI and emerging technologies as they impact our shared goals regulating for Online Safety.
- **We are closely monitoring developments in AI regulation overseas, and in international AI governance, that have the potential to impact UK citizens and industry.** In 2025, we joined UNESCO's Global Network for AI Supervisory Authorities, and we are following the development of other international regulatory networks in Europe, to better understand the practical implementation of the EU AI Act across the European region including for the UK (alongside sector-specific work in other networks including GOSRN and EPRA – see Annex 1 for more information).
- **We are also focused on relationship-building.** As global conversations develop between regulators on AI topics, we are actively identifying areas of overlap with other regulators and supervisory authorities including through the DRCF. We are focused on building relationships to support coordinated approaches where we anticipate this helping with specific regulatory challenges, including through sharing experiences, discussing regulatory tools, and co-operating on specific topics.
- **We are participating in discussions on AI standards** in standards development organisations including at the International Telecommunication Union (ITU), where Ofcom takes a leading role in representing the UK. Ofcom also participates in the European Telecommunication Standards Institute (ETSI)'s Technical Committee: CYBER, where the telecoms aspects of AI security are formalised. We work closely with the NCSC and AISI in following standards developments.

Our internal AI use

4.10 **This year we are focusing on identifying our foundational requirements to enable effective and safe AI adoption and use.** This includes strengthening our AI governance framework and improving the way we support and upskill our colleagues. We will continue to assess our business requirements and capabilities to ensure our approach to AI remains ethical and is aligned and supported by our ongoing data strategy.

4.11 **We are experimenting with how we can use AI to support our research, policymaking and internal processes**, including, but not limited to:

i) Testing a range of innovative new approaches in our policy work, including running pilots to explore how AI can play a role in supporting parts of the policy development lifecycle.
ii) Exploring how we could use AI to enhance our research – including by building and applying AI capabilities to augment our existing approaches.
iii) Developing our own AI tools and algorithms to help streamline our consultation process and to support our work in tracking developments in technical standards fora.
iv) Making our internal operational processes more efficient.

4.12 **Safety remains at the heart of our internal work on AI.** We will continue to trial how AI can support our policy and operational work, building on our work over the last few years. We are taking the time to ensure we continue to use AI in a safe, ethical, and secure manner by experimenting in small pockets before rolling this out more widely.

A1. Our planned AI work

A1.1 Ofcom's planned AI work will ensure that we continue to identify and respond to AI-related risks across our remit. This work 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.

A1.2 Ofcom's Plan of Work 2026/27 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 2026/27

Cross-sectoral	• We are focusing on identifying our foundational requirements to enable effective and safe AI adoption and use. We will continue to assess our business requirements and capabilities to ensure our approach to AI remains ethical and is aligned and supported by our ongoing data strategy.
	• We are experimenting with how we can use AI to support our research, policymaking and internal processes, including:
	  ○ Testing a range of innovative new approaches in our policy work, including running pilots to explore how AI can play a role in supporting parts of the policy development lifecycle.
	  ○ Exploring how we could use AI to enhance our research – including by building and applying AI capabilities to augment our existing approaches.
	  ○ Developing our own AI tools and algorithms to help streamline our consultation process and to support our work in tracking developments in technical standards fora.
	  ○ Making our internal operational processes more efficient.
	• We are exploring how Ofcom can improve our support for UK innovation by engaging proactively with entrepreneurs, startups, and SMEs.
	• We are carrying out research on trust and AI chatbots as part of our media literacy work. This is likely to include usage and attitudes in relation to AI chatbots, use of language and anthropomorphisation (the act of attributing human characteristics, behaviors, or motivations to non-human entities, such as animals, objects, or natural phenomena) and how language shapes understanding, trust and media literacy.
	• We will continue our horizon scanning work to identify emerging and longer-term AI developments that could have implications for citizens and consumers, regulated services and regulated sectors.

Policy area	Work we will do in 2026/27
	• We will continue to proactively monitor and engage with AI developments internationally, such as the EU's AI Act, to understand their impact on Ofcom's regulated sectors and stakeholders. • We are engaging in domestic and international regulatory forums, including the DRCF, the Global Online Safety Regulators Network (GOSRN) and the European Platform of Regulatory Authorities (EPRA), on AI issues that cross regulatory remits. • We will continue to engage on AI issues within standardisation bodies, including Ofcom's ongoing representation of the UK at the ITU.
Online safety	• We will continue to act within our powers to address harms exacerbated by AI such as deepfake intimate image abuse and synthetic child sexual abuse material (CSAM). We will take appropriate action where we identify non-compliance with the Online Safety Act, including launching investigations and taking other enforcement action. • Our internal OST Lab will continue to support practical research into safety technologies, allowing colleagues to investigate and demonstrate the extent and power of online safety technologies. • We are exploring the impact of GenAI on search engine experiences to produce a research paper, with technical support from the OST Lab. This builds on the publication of our most recent GenAI discussion paper, The Era of Answer Engines, which examined the impact of GenAI tools on the future of search engines and the long-term economic viability of news organisations, as well as implications for media literacy. • We will examine the implications of so-called 'AI companions' for online safety. We recognise there are many concerns about their potential to encourage unhealthy chatbot-user relationships and create harmful dependencies. This work will complement our research on trust and AI chatbots as part of our media literacy work. • We are building an enterprise data lake which includes Online Safety data, as well as data from other regulatory areas. This will build AI-readiness capabilities by describing and cataloguing reusable online safety data sets that can be used for machine learning and agentic queries. • We will monitor the development of new AI technologies, products and services, and make sure that services that use or deploy in-scope AI tools are aware of their obligations under the Online Safety Act. • We will continue to engage with the growing third-party AI Assurance sector over the coming year. These firms could work with online services to build trust and confidence in their AI systems. There may also be opportunities to support audits of AI systems against specific regulatory requirements.

Policy area	Work we will do in 2026/27
	• We will prepare for potential new duties and powers relevant to our online safety remit – following the Crime and Policing Act and the Schools and Children's Wellbeing Act – and work with the Government to ensure these are effective in further protecting users from harm linked to AI services. • We are a member of the Leadership Council of GOSRN, a growing network of regulators with responsibility for online safety. The focus in 2026 has been to tackle common challenges regulators face, including addressing AI-generated non-consensual intimate images and CSAM, and how to manage the challenges of GenAI.
Telecoms & Digital Infrastructure	• We are investigating the impact of AI on the customer's experience of the telecoms market, setting out the current and future effects. As part of this work, we have been engaging with industry through individual discussions and a roundtable. We plan to publish our findings in the second half of 2026. • We are seeking input from operators regulated under the Communications Act 2003 (as amended by the Telecommunications (Security) Act 2021 (TSA)) and the NIS Regulations 2018 to understand how AI is currently being used in cybersecurity and whether regulatory requirements may present unintended barriers to adoption. • We are investigating how AI is being applied, or could be applied, by telecoms providers to support network management and optimisation, including in areas such as fault prediction, and performance management. • We are investigating how networks could reliably support AI applications and AI-enabled services at scale. This includes understanding requirements relating to connectivity, capacity, performance, and coverage, and understanding where the market is likely to deliver through existing network assets, and where constraints may remain. • Building on our previous work in collaboration with Digital Catapult, we will continue to build our understanding of how AI can be applied in telecoms networks and explore what may be needed to support trustworthy AI adoption in telecoms networks. • Ofcom participates in ETSI's Technical Committee: CYBER, where the telecoms aspects of AI security are formalised.

Policy area	Work we will do in 2026/27
Broadcasting & Media	• We will continue to build our understanding of how AI is being used in UK broadcast, production and the wider media sector, and what is needed for safe, responsible adoption. • We are a member of EPRA, a network of over 50 European 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 looking at the use of Large Language Models (LLMs) to analyse content at scale, exploring the potential of LLMs to support our regulatory functions. The pilot project will focus on two use cases: the first being analysis of news content, and the second will be analysis of online content to support our prominence work.
Spectrum	• We are building a data lake for a range of spectrum licence information, structuring the underlying data sets to make them more accessible to industry and the public. We aim to prepare an infrastructure and clean datasets that can in future be used for agentic queries, to build our AI-readiness capabilities. • We are developing a proof-of-concept which is using AI/machine learning to assess occupancy in a localised set of ultra-high frequency (UHF) monitoring data. If successful, we will look to extend this work into other bands / geographies to further refine the process. • We will further our research work on the application of machine learning for radiowave propagation modelling across a range of scenarios.
Post	• We will continue to monitor how the postal sector could further embrace AI opportunities.

A2. Use of agentic AI across Ofcom's regulated sectors

A2.1 Over the past year, we have seen a growing interest in agentic AI within our sectors. Through our horizon scanning, we have identified many different agentic AI use cases across our sectors. For each use case identified, we considered the potential opportunities and risks to consumers and/or industry. It is worth noting for all use cases below that accountability and control could present challenges. Agentic systems are inherently adaptive and can make consequential decisions without direct human intervention. Without robust governance and meaningful human oversight, these systems, like all AI systems, risk becoming opaque "black boxes", making it difficult to explain or contest decisions made by agents.

A2.2 Our examples feature both current and future use cases, as our findings suggest that our sectors are at different stages of maturation in their use of agentic AI. We also note that some of the use cases which are technically possible are not yet widely adopted by industry – but this may change in the near future. We have indicated these stages and whether they are currently 'live', in 'pilot or proof of concept' or a 'potential future use case'.

A2.3 We have set out our findings in the table below. This overview is not intended to be a comprehensive list of every agentic AI use case within our sectors; rather, we are spotlighting the examples which have the greatest potential to transform the communications landscape.

Relevant sector(s)	Description of use case	Opportunities and risks for industry and consumers
Online	**No-code software development** – '*Live*' While earlier GenAI tools can write code, it requires a human to decide what to do with it, run tests, troubleshoot errors, and deploy changes; agentic AI can autonomously execute the whole code generation workflow. This involves the AI agent writing the code, running tests, identifying failures and iterating fixes, deploying and updating software – all without human intervention.	• **Software developers can deploy and upgrade new software** without requiring high technical capability, lowering barriers to entry for small firms or individuals. • **Faster delivery of software updates** may bring significant efficiency gains, saving developers time and money. **However,** • There is already evidence of no-code software development **enabling bad actors to independently automate cyber-attacks**. This in turn, could increase the number and efficiency of cyber-attacks. • **Risk of cascading errors without sufficient human oversight**. As AI agents carry out multi-step processes, if an agent makes an initial error or judgment, further errors may be triggered.

	Autonomous online content moderation – *'Live'* AI agents can scan user-published content and identify illegal or harmful content. This can either be flagged for human review or immediately removed by the agent.	• **Content moderation can be carried out at scale,** keeping pace with the rate of publication on large platforms. • **Faster removal of harmful or illegal content** may minimise the time in which users are exposed to problematic content. **However,** • **There could be impacts on freedom of speech** if an agent applies rules too broadly or incorrectly identifies lawful content as harmful. Therefore, there is a risk ofunnecessary restriction of lawful content. • **Higher autonomy can pose a greater risk of opaque or "black box" decision-making.** This can make it harder for service providers to understand why content has been removed or to justify their decision-making.
Post	**Procure and broker with freight transport providers** – *'Live'* AI agents can analyse cost availability and capacity across multiple freight providers. Agents can then autonomously negotiate and purchase their services on behalf of goods providers.	• **Makes cost-effective procurement decisions** reducing reliance on human freight desks. **However,** • **Risk of poor procurement decision-making** if agents select providers based on incorrect information or on narrow criteria such as cost, without considering other crucial factors such as reliability. This could result in a bad contract or service outcomes.
	Optimising postal delivery routes – *'Potential future use case'* Agentic AI may soon be capable of automatically re-routing delivery drivers through real-time analysis of traffic data and parcel requirements.	• **More efficient use of fleet** resulting in faster delivery times and lower costs. **However,** • **Risk of poor service delivery** if agents rely on bad quality or incomplete data for decision-making. This could result in delays or reduced services. • **Preservation of driver well-being.** If systems overly prioritise efficiency over welfare, this may have a negative impact on drivers.
Broadcasting & Media	**Dynamic pricing of audiovisual content** – *'Live'* AI agents can automatically price content when broadcasters and creators sell	• **Enabling faster reuse, selling and distribution** of content helps creators share it more widely and increase monetisation opportunities.

	clips to third parties (e.g. advertisers or news outlets). Price points are set through analysis of content and real-time data about commercial context.	• **Saves time** through reducing the effort of manually setting prices and reviewing rights management protocols. **However,** • **Risk of opacity over pricing decisions** for buyers and creators. A lack of clarity around how agents negotiate could make it harder to understand if decision-making has been fair.
	Recommend personalised media and content across platforms – *'Pilot'* Recommendation systems are now integrated into many television devices – using AI to search across multiple apps and platforms and list recommendations based on users' personal and contextual data. While there are not yet any fully agentic recommender agents capable of continuously curating and updating choices unprompted, systems rapidly mature.	• **Provides a more personalised and accessible viewing experience** for users. • **Reduces friction in users' content discovery experience**, with the potential for higher customer engagement and retention for media providers. **However,** • **Personalisation of content may reinforce 'echo chambers',** and limit exposure to a broad range of content. This could ultimately undermine the benefits around discovery that agents were intended to support. • **Commercial incentives may limit the rollout** if content platforms are reluctant to allow external agents to use their services, especially if it means external agents acting as gatekeepers between providers and their audiences.
Telecoms	**Telecommunications network optimisation and maintenance** – *'Potential future use case'* Agentic AI could build on existing closed-loop automation to continuously monitor network traffic and, within pre-defined guardrails, dynamically adjust network parameters (such as bandwidth allocation) during demand peaks. It could also support network assurance by analysing network signals (such as alarms), reason over real-time and historical network data,	• **Faster detection and resolution of faults** could help improve service quality and internet reliability, benefiting both business and individual telecoms customers. • **Continuous optimisation of infrastructure deployment** could help prevent unnecessary duplication of assets, saving money and using fewer resources. • **Deploying AI in networks to more efficiently manage infrastructure and energy use** could improve sustainability in future, both by reducing emissions from power usage and by lowering energy costs for network providers. **However,** • **Applicability to critical national infrastructure** means risk of cascading

	and trigger appropriate remedial actions – such as reconfiguring network settings or rerouting network traffic for well understood and repeatable scenarios, while retaining human oversight for higher-risk interventions.	errors will have a higher impact, while adoption may be slower. • **It may be difficult to explain why a specific decision was made**, creating potential challenges related to incident reporting.
Spectrum	**International spectrum standards development –** *'Potential future use case'* Agentic AI could support the development of standards to enable consistent and agreed spectrum management.	• The **cross-border, international nature of spectrum** requires standards **adherence** and **harmonisation** to **avoid interoperability issues** and help enable economies of scale. • **Agentic AI could help streamline the complex process** of international spectrum standards development. **However,** • **Highly technical & numerical aspects of spectrum management** will require further AI model development. • The wide span of spectrum characteristics (from Hz to GHz) **requires a range of approaches**, not one-size-fits all.
Cross-cutting	**Administrative task automation** – '*Live'* AI agents are being deployed across the communications sectors to automate routine administrative tasks like: taking and summarising meeting notes; helping creative ideation; and managing inventory by analysing demand data and automatically reordering stock for e-commerce.	• Increased automation **frees up staff to focus on higher-value and more engaging work**, potentially leading to better employee satisfaction and outputs. • While integration of agents has been incremental, as a use case it's perceived as lower risk, likely meaning that **adoption will be sustainable with cumulative efficiency gains made**, with **reduced operating costs** across the organisation. **However,** • High trust in AI outputs could **lead to poor operational decision-making** based on inaccurate or incomplete data.
	Agentic customer service chatbots – *'Pilot'* Agentic AI chatbots are not only capable of responding to customer queries, but they can also independently interpret and resolve them. These chatbots could be capable of carrying out actions	• Agentic AI chatbots can provide instantaneous responses, providing **faster and often more effective resolution of queries**, which overall could **improve customer satisfaction.** • Efficiency gains and reduced pressure on often overstretched customer service staff may result in **reduced operating costs and higher staff satisfaction**. **However,**

	such as enacting a refund or cancelling an order. Although deployment of agentic AI chatbots is currently limited, we anticipate there will be wider adoption within our sectors in the near term.	• Some evidence indicates **consumer scepticism around chatbot interaction** and their effectiveness, with a preference for human engagement.
	Enhanced cybersecurity vulnerability testing – *'Live'* Agentic AI vulnerability testers can deploy AI agents to operate without human intervention to analyse a 'software target', coordinate agents to devise simulated cyber-attacks, and identify and report vulnerabilities. Agentic AI can also be used for threat responses by monitoring alerts and executing appropriate responses.	• Autonomous vulnerability testing and threat responses could **provide faster identification of vulnerabilities and responses to incidents**, improving resilience against increasingly sophisticated attacks. • **Facilitates deployment of cybersecurity responses without the requirement of high-level cybersecurity expertise**. With a dearth of cybersecurity skills globally, agentic interventions address these issues. • Security operatives are often required to provide round the clock threat monitoring, so doing some of this autonomously **helps alleviate staff burn out and reduces workload.** **However,** • **Same tools are being used by bad actors to independently automate cyber-attacks.** This, in turn, could increase the number and efficiency of cyber-attacks, raising overall threat level.