

Report of the Online Information Advisory Committee, October 2026

A requirement under s.152(5) of the Online Safety Act

13 October 2026

About this report

The Online Information Advisory Committee was established by Ofcom to fulfil its duty under section 152 of the Online Safety Act ('the OSA') to establish and maintain an advisory committee on disinformation and misinformation. We describe the legislative framework and history below.

The Act provides that the Committee must publish a report within the period of 18 months after being established. The Committee is publishing this report to fulfil that duty. The Committee, and not Ofcom, is responsible for the content of this report. We publish other reports and the minutes of our meetings, and an overview of the work we have done so far is set out below.

The members of the Committee were appointed through the process that Ofcom uses for a range of its statutory bodies. Committee members serve as individuals rather than as representatives of any organisation.

The Act does not specify the purpose, content, or audience of the report. However, the Committee has a specific role prescribed by the Act and this report reflects that role. We stress that this is not a general report on disinformation and misinformation as they affect the UK, or on the OSA. However, as the duty to report was also prescribed by Parliament, we have tried to share conclusions from our work that will be helpful to parliamentarians and others involved in policy making in this area where we can within our remit. We welcome any feedback that can inform the Committee's future reports.

Defining disinformation and misinformation

The UK Government has defined disinformation as the deliberate creation and spreading of false and/or manipulated information that is intended to deceive and mislead people, either for the purposes of causing harm, or for political, personal or financial gain. Misinformation is defined as the inadvertent spread of false information.¹ Similar definitions are used elsewhere. Although the distinction based on intention is important, disinformation and misinformation are inseparable: if you deceive me and I repeat your lies, your disinformation becomes my misinformation.

Put as simply as possible, disinformation and misinformation mean deceptions and mistakes. It can sometimes be helpful to use simpler language to encourage clear understanding and proportionate responses to the issues involved. Asking what Ofcom is doing about online misinformation would be much the same as asking what Ofcom is doing about people making mistakes on the internet. Putting it in the simpler language helps show that a clearer and more focused problem statement is needed if we are to have a proportionate and effective response.

Disinformation and misinformation are features of open societies. They cannot be eliminated because the measures needed to eliminate them would be the end of an open society. But they are not abstract problems. Disinformation and misinformation cause and contribute to specific problems

¹ See, for example, Cabinet Office and Department for Science, Innovation and Technology, 2023. [Fact Sheet on the CDU and RRU](#). As quoted in Communications and Digital Committee, 2024. [The Future of News](#), chapter 7.

for specific people and there is good, focused work to be done protecting people from specific categories of harm—from financial fraud to foreign interference.

Freedom of expression

Freedom of expression is central to the Committee's work. There are real threats from disinformation and misinformation but perhaps even greater threats from overreacting or reacting inappropriately to those threats. Our commitment to freedom of expression drives our work to clearly define real problems and proportionate solutions within our remit of disinformation and misinformation. We emphasise that in the UK's legal framework, freedom of expression includes the freedom both to impart and to receive ideas. The importance of freedom of expression is also a key theme of the OSA. Our role includes advising Ofcom on how its work in this area can best respect and protect freedom of expression and be proportionate to the risks involved. We will return to this theme throughout the report.

Alongside the legal right to freedom of expression is a simple respect for people's ability and right to make up their own minds. Prof. Sir Chris Whitty, Chief Medical Officer, has recommended "countering disinformation about vaccines forcefully when necessary"² but also observed that "the British public are actually extraordinarily sensible on almost all of these topics... and we need to remember that."³

Legislative context

The original Online Harms White Paper in 2019 proposed that: "Companies will need to take proportionate and proactive measures to help users understand the nature and reliability of the information they are receiving, to minimise the spread of misleading and harmful disinformation and to increase the accessibility of trustworthy and varied news content."⁴

The Committee was first proposed in the Draft Online Safety Bill published in 2021 where it was paired with powers for Ofcom to regulate content where there was a "risk of the content having, or indirectly having, a significant adverse physical or psychological impact on an adult of ordinary sensibilities."⁵ It was expected that this new category of regulated content would include various types of disinformation and misinformation.

The powers to regulate so-called 'legal but harmful' content in general, including disinformation and misinformation that did not amount to a criminal offence, were taken out of the Bill in late 2022 but the advisory committee was maintained into the final text of the Act that was agreed in 2023. The

² For example, in Chief Medical Officer, 2025. [Chief Medical Officer's annual report 2025: infections, Executive summary and recommendations](#).

³ Professor Sir Chris Whitty, 2026. [Prof Sir Chris Whitty on disinformation and misinformation in health care: Summit 2026 session](#), at 13m20s.

⁴ HM Government, 2019. [Online Harms White Paper](#), p. 71.

⁵ HM Government, 2021. [Draft Online Safety Bill](#), p. 41.

Committee has had to consider how it can best provide advice to Ofcom given this evolution of the legislation away from providing the regulator with as many substantive powers in this area.

In setting an agenda for the Committee we have tried to be true to both the broad statutory goal of the adequate protection of citizens from harm, and to the letter of the statute and the specific powers and duties it gives to Ofcom.

Warnings on disinformation and misinformation in the UK

There is a high level of interest in this topic from a wide range of important expert voices in public life and in particular from national security leaders. The Committee is committed to drawing on the available evidence base to inform our advice.

Before we explain Ofcom's narrow role in relation to disinformation and misinformation, it may be helpful to bring together some of the stark official warnings of the threats from disinformation and misinformation at national and international level.

The Rycroft Review into countering foreign financial influence and interference in UK politics concluded: “My assessment, then, is that we are, indeed, already experiencing ‘information warfare’. While our political life has not yet been subsumed by this assault, our defences are worryingly weak. If relentless exposure to disinformation on social media persuades even a small proportion of the UK population that our politics is irretrievably broken, the risk grows rapidly that some will seek to resolve their discontents by extra-political action.”⁶

The Chief of the Secret Intelligence Service, MI6, has warned: “We are being contested from sea to space, from the battlefield to the boardroom. And even our brains, as disinformation manipulates our understanding of each other and ourselves. Across the globe, we are now confronting not one single danger, but an interlocking web of security challenges – military, technological, social, ethical even – each shaping the other in complex ways. We are now operating in a space between peace and war.”⁷

The Chief of Defence Staff⁸ and previously the Director General of MI5 in 2024⁹ have also warned about disinformation. The Government’s media literacy strategy states that “the spread of misleading information online contributed to unrest in our communities” in the aftermath of the Southport attack.¹⁰ The Foreign Affairs Committee of the House of Commons has concluded that

⁶ The Rycroft Review, 2026. [The Rycroft Review: Report of the Independent Review into Countering Foreign Financial Influence and Interference in UK Politics](#), p. 19.

⁷ Blaise Metreweli, Chief of the Secret Intelligence Service, 2025. [Speech by Blaise Metreweli, Chief of SIS, 15 December 2025](#).

⁸ Air Chief Marshal Sir Richard Knighton KCB ADC FREng, 2026. [Chief of Defence Staff Speech at London Tech Week](#).

⁹ Director General Ken McCallum, 2024. [Director General Ken McCallum gives latest threat update](#).

¹⁰ Department for Science, Innovation and Technology, 2026. [A Safe, Informed Digital Nation](#).

“disinformation and foreign information manipulation and interference (FIMI) should be viewed as an existential threat to the UK and its interests overseas.”¹¹

We respect the expertise and authority of each of these institutions, and we draw attention to their warnings. We welcome the commitment in the Defence Investment Plan to a national conversation on defence and security,¹² which needs to include informed discussion on disinformation and misinformation, foreign interference, and the full range of possible responses, not just those that would fall to Ofcom. We recognise that informed public debate is complicated by the amount of low-quality research and analysis in this area, and in particular analysis which seeks to attribute disinformation and misinformation activity to hostile state actors based on flimsy evidence. The threat is real, but many claims made about it are not. In our view this underscores the value of an informed national conversation on these issues.

These warnings are necessary to understand the context of the Committee's work and Ofcom's work. However, Ofcom must work within the specific role and powers parliament has given it, using open evidence to inform its decisions, and respecting and protecting freedom of expression. Broad statements of the risks such as these are important, but regulatory action has to be targeted and proportionate based on the law and the evidence.

The National Risk Register does not include disinformation and misinformation among its list of the most serious risks facing the UK.¹³ It does recognise that in some cases disinformation and misinformation can exacerbate other risks, and the 2026 register includes a new risk of interference in UK democratic process, which it says could include “deterioration of the online information space”.

In the Committee's work, we have tried to take a similar approach of seeking to understand specific harms that can be caused or worsened by disinformation and misinformation, and proportionate responses to those risks.

Ofcom's role in relation to online disinformation and misinformation

The legislative framework governing Ofcom's work on online disinformation and misinformation is complex. What follows is not intended to serve as a complete statement of the law.

Parliament decided to give Ofcom few specific powers and duties in relation to online disinformation and misinformation. Under the Act, Ofcom does not have any direct powers to require companies to act on misinformation or disinformation as they are not defined as illegal content, or content that is harmful to children under the Act. There are some related powers that are tangential to these issues and could help counter online disinformation and misinformation, but these only apply in very

¹¹ Foreign Affairs Committee, 2026. [Disinformation diplomacy: How malign actors are seeking to undermine democracy](#), p. 3.

¹² Ministry of Defence, 2026. [The Defence Investment Plan: Equipping our forces, defending our future](#).

¹³ HM Government, 2026. [National Risk Register 2026](#).

specific circumstances. Some may amount to a priority or non-priority illegal offence, such as fraud offences, the foreign interference offence, and the false communication offence. The bar for reaching the criminal threshold is high, and some offences, for example with foreign interference include content beyond disinformation and misinformation. Some disinformation or misinformation may also overlap with categories of content harmful to children as defined in the Act.

Ofcom also has related duties that may have an effect on preventing the spread of disinformation or misinformation. These include the additional duties on categorised services to apply their Terms of Service consistently, since some services have policies prohibiting or demoting certain forms of disinformation or misinformation.

In addition, there are media literacy duties on Ofcom, but not on regulated services, in relation to misinformation and disinformation. There is also a statutory requirement to create and maintain the advisory committee focusing on disinformation or misinformation. Beyond these related powers, Ofcom does not have any other powers related to disinformation or misinformation under the OSA.

Illegal content under the OSA

However, where such content amounts to a relevant offence, or intersects with a type of content set out in the Act that is harmful to children, the duties on providers will apply. In section 59 of the OSA, parliament created a category of "illegal content" meaning content whose use, possession, viewing, accessing, publication or dissemination amounts to a criminal offence, other than certain types of offences specified in subsection 6, such as intellectual property offences.¹⁴ Regulated services have duties in relation to illegal content.

Duties apply in relation to illegal content that relates to a specified "priority offence" such as foreign interference which broadly aim to prevent or minimise the risk of individuals encountering priority illegal content. Specified priority offences set out in Schedule 7 that may connect with disinformation and misinformation include fraud and financial crime, hate and harassment, and foreign interference. As the next section sets out, the Committee has programmes of work relevant to each of these areas.

Terms of Service duties for categorised services

In addition to the requirement on user-to-user services to ensure that they apply their own Terms of Service consistently in respect of illegal content and content harmful to children, in the future, Category 1 services will have additional duties to apply Terms of Service consistently in relation to restricting users' access to content or suspending or banning users. This includes where they have policies related to disinformation or misinformation.¹⁵ There is no requirement on services to have such policies, but where they exist, service providers will need to apply their Terms of Service consistently.

¹⁴ The precise wording is set out in the [Online Safety Act 2023, section 59](#).

¹⁵ The precise wording is set out in the [Online Safety Act 2023, section 72](#).

Transparency duties for categorised services

The OSA gives Ofcom powers to issue annual transparency notices, which require providers of categorised services to publish transparency reports containing information about specified online safety matters. These reports are intended to improve the public's understanding of online safety risks, the measures providers take to address them, and wider industry trends in online safety. Ofcom must also publish its own annual transparency report drawing on information produced by providers about their services. The Committee is required to advise on the exercise of these powers insofar as they relate to misinformation and disinformation. We discuss our work in this area below.

Media literacy duties for Ofcom

The Act clarifies and adds specificity to Ofcom's existing media literacy duties. The Act states that: "OFCOM must take such steps, and enter into such arrangements, as they consider most likely to be effective in heightening the public's awareness and understanding of ways in which they can protect themselves and others when using regulated services, in particular by helping them to... understand the nature and impact of disinformation and misinformation, and reduce their and others' exposure to it."¹⁶ The Committee is required to advise on Ofcom's exercise of these functions in relation to countering disinformation and misinformation on regulated services and we discuss the work we have done below. The Act does not place any corresponding duties on regulated services.

The work of the Online Information Advisory Committee so far

Section 152 of the OSA states that the Committee must provide advice to Ofcom on:

- a. how providers of regulated services should deal with disinformation and misinformation on such services,
- b. OFCOM's exercise of the power conferred by section 77 to require information about a matter listed in Part 1 or 2 of Schedule 8, so far as relating to disinformation and misinformation, and
- c. OFCOM's exercise of their functions under section 11 of the Communications Act (duties to promote media literacy) in relation to countering disinformation and misinformation on regulated services.

The Committee aims to be led by research and evidence. Our main outputs are a series of published advice notes and literature reviews on protecting people from specific types of harm caused or contributed to by disinformation and misinformation. In addition, the Committee also advises on Ofcom's work as appropriate. Minutes of our meetings are published on the Ofcom website.

The first advice note was published in November 2025 and focused on financial disinformation. The second advice note was published in October 2026 and focused on certain online threats to

¹⁶ Further detail can be found in [Online Safety Act 2023, section 165](#).

elections. The third advice note, currently in preparation, will focus on online disinformation and misinformation and offline public disorder.

In addition to these advice notes, the Committee has also engaged with Ofcom on a range of other topics. These include:

- The foreign interference offence
- Ofcom's work on media literacy as it relates to online misinformation and disinformation
- Researcher access to data
- Elections, including on Ofcom's work ahead of the May 2026 elections
- Engagement with the Electoral Commission
- Women and Girls' Online Safety
- Behavioural insights research
- Ofcom's Online Safety work related to technology
- The exercise of Ofcom's transparency powers

The Committee intends to continue publishing advice notes supported by high-quality evidence on specific areas where there is concern that disinformation and misinformation cause or contribute to harm relevant to the Committee's remit. These may include:

- Foreign interference
- Radicalisation and countering violent extremism, specifically the mechanisms of radicalisation where relevant to the Committee's remit
- Health-related harms
- Women and Girls' Online Safety
- AI-generated content and its impact on misinformation and disinformation
- How peoples' perceptions of risks can be impacted by misinformation and disinformation

Transparency and information requirements

This work is ongoing. Under the Act, the transparency requirements for categorised services could only come into effect once the categorisation register was established. This committee's general view is that the information, data, and evidence that are openly available are insufficient as a basis for effective policy making and operational decision making on disinformation and misinformation and this is reflected in our comments on the evidence base below. In line with our statutory duties, by the time of publication the Committee will have reviewed and given feedback on the sections of the transparency notices that relate to disinformation, misinformation, and media literacy.

Media literacy

The Committee met with Ofcom's Making Sense of Media team in our second meeting in June 2025 and provided input into [Online Safety: Our Research Agenda](#). Because Ofcom lacks powers to compel platforms to implement its media literacy recommendations, it is imperative for platforms to implement them voluntarily. In addition, we have recommended that Ofcom should use its

transparency powers to compel platforms to disclose information on their own efforts to promote media literacy.

Artificial Intelligence

The new generation of billion user online services are Artificial Intelligence (AI) tools, currently focused on text-based chat but extending far beyond that. Some of these tools are captured under the Act's definition of user-to-user or search services, but not all of them. We understand that Parliament will be considering how to extend and adapt the illegal content safety duties in the OSA to include AI services via secondary legislation, outlined in a delegated power in the Crime and Policing Act 2026.¹⁷

In our advisory note on elections, we recommended that Ofcom should encourage and commission research into the use of generative AI as a source of political news and opinion by young and first-time voters, whose importance will grow sharply if the franchise is extended while access to some services may be restricted, in line with the UK Government's announcements to ban under 16s from social media. It should also encourage and commission research into private messaging services. We note that Ofcom has published its [News Report 2026](#), showing that one in five adults are now using AI tools to keep up to date with the latest news.

The existence of these new technologies raises new issues in relation to disinformation and misinformation, including reducing the cost of producing and personalising multimedia and multilingual disinformation content to trivial levels.

A further, emerging concern is the use of agentic AI systems capable of planning and executing multi-step tasks with limited human oversight, which could in time automate not only the content of disinformation campaigns but their coordination and adaptation as well. We recommend that Ofcom's media literacy and research functions should treat this evolving capability, rather than any single current technology, as the relevant and durable object of ongoing attention.

Existing capabilities are sufficient to worsen harms caused or contributed to by disinformation. A prudent assumption is that the risks will become significantly more severe and the opportunities available to hostile actors will become significantly greater.

Ofcom's media literacy and research functions should also consider how the same capabilities that lower the cost of producing disinformation can also be applied against it. For example, in detecting synthetic or coordinated content at scale, verifying the provenance of images and video, and adapting and translating media literacy resources for different audiences more cheaply than has previously been possible.

¹⁷ Parliamentary Question on [Artificial Intelligence: Safety](#), 2026.

For those defending against malicious disinformation and committed to protecting freedom of expression, limitations in the existing framework are likely to have more severe consequences as hostile actors exploit AI for disinformation.

There is overlap between AI providers and providers of regulated services under the OSA, but if any new providers are brought into scope via new secondary legislation that extends the illegal content duties to AI services they will encounter challenges familiar to those already tackling harms from disinformation and misinformation on their services: the lack of operational and legal definitions, the lack of clarity about the remits of different actors with relevant responsibilities, the lack of powers and duties around information sharing, and so on. Similarly, AI will highlight the limits of Ofcom's powers around for example requiring platforms to take action to promote media literacy, ensuring users' access to authoritative information, and visibility of AI content.

Insights for decision-makers beyond Ofcom

There are some lessons from the Committee's work that inform our advice to Ofcom but go beyond Ofcom's purview. We share these points in the hope that they may be of use to the relevant decision makers, in the light of warnings from national security leaders described above. In the course of working very closely with Ofcom over the last 18 months, we've observed a number of challenges that are often framed as ones for Ofcom to solve that we understand are either dependent on other organisations or go beyond Ofcom's regulatory remit. We want to highlight where there is greater need for coordination or to highlight more clearly where those misconceptions lie.

1. Need for greater understanding of the decisions Parliament and the UK Government have made in relation to disinformation and misinformation.

Concern about disinformation is often most acute during and after a major incident and it is natural that under these circumstances, there will be urgent calls for action from bodies seen as having relevant responsibilities. In these circumstances especially, political leaders have an important role in ensuring that what is asked of Ofcom is within the powers and duties given to it by the OSA.

We have tried to set out in this report the specific and limited powers and duties Ofcom has in relation to disinformation and misinformation under the OSA. Before the May 2026 elections, Ofcom wrote a helpful [open letter](#) explaining its role in relation to them. We note the importance of Ofcom continuing to explain its role under the OSA without taking on the role of advocating for or defending the Act. It is also important to stress that while disinformation is both an online and an offline phenomenon, Ofcom's role under the OSA only applies to online information, so it is inaccurate to suggest that Ofcom has general duties in relation to disinformation or misinformation.

2. Election preparedness.

Countering disinformation targeting elections is vital for our democracy. It is equally vital for that work to be trusted by the electorate.

Right now, it is unclear what would happen if a credible threat to an election was detected, what the role of politicians seeking election would be in response, whether potentially classified information

would be shared as needed, whether the relevant bodies are prepared to collaborate under time pressure, and whether the response would be effective.

The simple and practical precaution needed is the publication of a high-level statement like Canada's Critical Election Incident Public Protocol of how a credible election threat would be handled.¹⁸ The committee was initially minded to include this as a recommendation to Ofcom in our Advice Note on elections but it is clear that it would not be Ofcom's role to lead on this.

Government, Parliament, and national security leaders have repeatedly warned the public that there are credible threats to our democracy from disinformation. They have not said what they will do about them. Without setting clear expectations for the public on what will happen in the event of a credible threat, there is a risk that claims of interference in elections, even based on flimsy evidence, will impact trust in the electoral process. Without clear roles, expectations, and information sharing processes for responsible bodies, there is a risk of having to improvise a response under political direction in the middle of an election. This would jeopardise public trust.

3. National security.

National security risks from disinformation are increased by the lack of information sharing, coordination, and clarity about roles with dispersed responsibilities. We believe this merits urgent consideration and where possible change. Information about threats needs to be shared in a way that can be acted on by both Ofcom and regulated services. It is hard to see how an open society can effectively resist harm from disinformation when vital diagnostic information is classified and not available to relevant public bodies, let alone the public.

4. Enabling cross-service action.

Risks from disinformation will often spread across regulated services, and between online and offline channels. Offline disinformation is not within scope of the OSA. In some areas of online safety, such as Counter Terrorism and Fraud, there are mechanisms for collaborating to reduce harm to users. These areas are covered by clearer legal definitions and responsibilities which do not exist in the case of disinformation and misinformation. We are aware of more ad hoc information sharing about risks and responses in the context of major events such as the pandemic or elections that has shown that these kinds of mechanisms can be valuable. Any such mechanism should be designed to reach service providers of all sizes: smaller and newer services often have the least capacity to independently identify and assess disinformation risks, even though those risks are not confined to the largest platforms.¹⁹ Consideration should be given to the value of promoting better cross-service understanding of risks and responses either in the context of specific risks such as elections, or on an ongoing basis.

5. Need for better evidence on disinformation and misinformation and their impacts.

¹⁸ Government of Canada. [Critical Election Incident Public Protocol](#).

¹⁹ Ofcom, 2025. [Helping small services navigate the Online Safety Act](#).

The research base on disinformation and misinformation, how they work and what impact they have, is limited and often low quality. Disinformation is an adversarial and dynamic risk which needs to be studied with appropriate methods and data to produce timely and useful results. The way that academic research is typically commissioned and funded on multiyear timelines seems to be an impediment to obtaining the actionable research needed. As we found in our Advice Note on elections, “For many widely discussed threats there is little or no high-quality evidence.”²⁰

We note the report of the Social Platforms Data Access Taskforce on Improving research access to social media data which states: “researchers in the UK are currently unable to obtain this data reliably, lawfully or at scale. Without it, the harms the Online Safety Act was designed to address cannot be independently measured or verified and the effects of platforms’ efforts to address them cannot be assessed. Nor can the effectiveness of the UK’s own regulatory regime be fully tested.”²¹ We agree. Similarly, Ofcom’s ongoing work on transparency has a role to play here.

6. Need for coherence in the legal and institutional framework.

Bringing a law as complex as the OSA into operation inevitably reveals areas where different responsibilities and work do not join up perfectly. Some examples we have become aware of relating to disinformation and misinformation, and some possible responses, include:

- a. There are media literacy duties on Ofcom but not on regulated services. The duty on Ofcom includes a duty in respect of disinformation and misinformation. Media literacy is an important opportunity for content-neutral, freedom of expression respecting defence against harm from disinformation and misinformation. Because Ofcom lacks powers to compel platforms to implement its media literacy recommendations, it is imperative for platforms to implement them voluntarily. Ofcom should use its transparency powers to compel platforms to disclose information on their own efforts to promote media literacy.
- b. Illegal content duties are triggered by criminal offences. Understanding how those offences apply in different circumstances sometimes requires specialist knowledge or judgement that belongs to another body. For example, we believe it would be helpful for the Electoral Commission to set out its view of how offences under electoral law should be interpreted in the context of the OSA, so that Ofcom and regulated services could act on that basis.
- c. Section 175 of the OSA provides for the Secretary of State to give directions to Ofcom in the event of a threat to the health or safety of the public, or to national security. The directions can require Ofcom to require regulated services to make a publicly available statement about the steps they are taking. This could be a routinely used power of real value, but it has not yet been used. One plausible example of a threat to national security would be an attempt to interfere in an election, and it is clearly not desirable for a Secretary of State who is a candidate in that election to improvise the first use of this power under those circumstances.

²⁰ Online Information Advisory Committee, 2026. [Understanding online information-based threats to elections](#).

²¹ Dr Alexandra Boutopoulou, Professor Katharine Dommett, Professor Amy Orben, Mark Scott, Dr David Zendle, 2026. Social Platforms Data Access Taskforce Final Report, September 2026, [A year of evidence: insights and recommendations on social media data access for research into online harms](#).

For both reasons, we suggest that it would be useful for the Secretary of State to ask Ofcom to advise on the circumstances in which it would be useful for this power to be exercised.

- d. The Committee is tasked with advising Ofcom on “how providers of regulated services should deal with disinformation and misinformation on such services” but it is unclear to us how regulated services can accurately make the nuanced, fact specific decisions based on specific criminal offences the Act calls for at internet scale. Unless Parliament addresses the question of how offences designed for enforcement through the courts are to be operationalised as to comply with the duties, in practice regulated services may choose to adopt Terms of Service that are broader than the criminal offences and enforce those. It is important that Parliamentary scrutiny of the Act recognises that the precise definitions of offences covered by the Act are not necessarily what drives operational decision making, and that safeguards that protect freedom of expression in the definition of criminal offences may not necessarily have the same effect in the context of the Act.

We are also concerned that there is a risk of incoherence in the statute book where the planned legislation to lower the voting age to 16 will connect with the child safety duties in the OSA. There is an opportunity for Parliament to address this during the passage of the Representation of the People Bill.

7. Cooperation between regulators.

Ofcom has an established process for working with other UK regulators through the Digital Regulation Cooperation Forum. As we said in our Advice Note on understanding online financial harm, joint work to look at the intersection of online safety, data protection, and financial services regulation would help with understanding how these regimes can be made to work together in the public interest to mitigate against false or misleading financial information. Similar joint work will be needed in other fields. Ofcom’s role under the OSA requires support from other regulators sharing information and expertise. Given that the division of powers and responsibilities between public bodies is decided by Parliament, Parliament may wish to monitor whether the intersections are working as it would wish.

Proposal for a National Centre for Information Defence

Since the preparation of this report, the UK Government announced its intention to establish a National Centre for Information Defence. This provides a potential opportunity to take action informed by points raised in this report, including in particular the need for effective information sharing and for election preparedness.

Freedom of expression is fundamental to an open society, and any action to counter disinformation must protect it. New initiatives in this area are rightly subject to scrutiny because of the risks they can pose to freedom of expression, and they can themselves become the subject of disinformation. For both reasons, it will be important for any new centre to be carefully designed, carefully explained and carefully scrutinised, with protections for freedom of expression built in from the outset.

Acknowledgements

The Committee has now worked with the staff of Ofcom for 18 months. They are exceptional public servants, and we are very grateful to them for their outstanding work in this challenging area, as well as across the whole remit of online safety and giving effect to parliament's decisions in the OSA. Ofcom is fortunate to have a team with the vision, expertise, and skill they bring to this work. We thank them all.

Mark Scott served as a member of the Committee, and Richard Allan served as chair of the Committee, from the beginning of our work together. Mark Scott stepped down in February 2026, and Richard Allan stepped down in July 2026. They were highly valued and expert colleagues who made essential contributions both to the content of the Committee's work and to the experience working with the Committee. We thank them both.