Your response

Question	Your response
Question 1: Do you have any comments on Ofcom's proposed Work Plan for 2026/27?	See following pages for our full response

Please complete this form in full and return to planofwork@ofcom.org.uk

fipr foundation for information policy research

Foundation for Information Policy Research response to Ofcom's proposed Plan of Work for 2026

5th February, 2026

1. Overview and summary list of recommendations

Our contribution seeks to offer technological, legal and policy expertise that can inform the work plan content as set out, work that may fall into scope in the near term following recent government announcements and horizon scanning for emerging issues, and work that may be missing from the scope. We outline key challenges for 2026-27 in relation to AI and communications services, emerging cross-jurisdictional flashpoints, age checks with regard to user-to-user regulated services, and debate and policy on social media and children. Across these policy areas, we suggest that Ofcom engage in further consultation with technical expert groups, including FIPR, on the benefits and negative consequences of potential technical designs, and what is possible - in technical terms - for the implementation of desired government policy, rather than leaving crucial decisions in the hands of industry or for post-legislative implementation.

To that end, we recommend that Ofcom:

1.1 Should not seek to extend the mandate of 'accredited technologies' but rather regulate for the desired outcomes. Evaluate the outcomes and assessing "whether life is getting safer online" therefore must include a range of evidence including the unintended consequences for individuals and communities where access to information or secure services (such as encryption and VPNs) is restricted in the name of "safety".

1.2 Consult on the effectiveness and accuracy of its definition and methodology of what "safer online" means, how it is measured, and for whom, to make this evaluation of impact, prior to undertaking the assessment itself.

1.3 Engage in further consultation with technical expert groups, including FIPR, on the benefits and negative consequences to privacy, security, and civic rights, of potential designs - to verify the design, validate the implementation, and plan how to monitor the operation of technical solutions relating to upload filters, hash matching, measures on-device, and encryption workarounds, rather than leaving implementation and self-assessment to industry alone.

1.4 That the workplan be expanded to include an independent audit to determine whether the efficacy assessment criteria and measures in practice are themselves effective, accurate, robust, relia-

ble, and fair, and to measure and evaluate their impact. This should be carried out on a periodic basis to ensure that understanding of the performance metrics remain reliable in step with changing and emerging technology.

1.5 Seek urgent and ongoing engagement with the wider applications of age assurance and verification, for broader consideration of other commercial environments, and civil society expertise on its changing technical architecture, development and application.

1.6 Commission further research work and consultation on the technological evidence of approaches to age assurance and age verification prior to any assessment of efficacy and its evaluation.

1.7 Take forward a stream of research work exploring the role that platform technologies play in harm to children, building on the wealth of academic and practitioner expertise on these topics in a UK regulatory context.

1.8 Develop a strand of exploratory work and mapping exercise on digital sovereignty.

1.9 That the scoping and horizon scanning of likely and emerging issues forms a larger part of the workplan and includes closer collaboration with leading academics and civil society. Concretely, Ofcom needs an Early Warning System built into its institutional infrastructure. This should include the establishment of a fast-track mechanism allow informed bodies and individuals to inform and engage with the regulators for such matters, and assign responsible case owners within the most appropriate regulator(s) and timeframes for responses.

2. We live a safer life online"[1]

We make a number of observations and recommendations on the provisions in the work plan relating to *safer experiences for children* and *platform regulation*. The work of implementing current government policy in this area faces a number of serious challenges. There is still a large gap in understanding of the role technology plays in crimes that harm children and minors, as well as of wider harms to young people that have a technologically-mediated component. Current policy approaches under the Online Safety Act create difficult conditions for tackling these issues, placing considerable power in the hands of technology providers to implement solutions, doing little to actively regulate the business models which are a key source of harms, and generally assuming that innovation can circumvent the constraints in material design and economic incentives posed by any policy 'ask'.

2.1 Duties on categorised services and Tackling harms at the source

> *"Ofcom aims to publish the final categorisation register and consult on additional duties (including those on fraudulent advertising, terms of service, user empowerment, ID verification, and content-related protections) in Q2 2026/2027 (2.22, p.15)*
>
> *[Ofcom] are proposing the expanded use of proactive technologies, such as hash matching to block known illegal images, and automated tools to detect harms or for child protection during livestreams. (2.22, p.15)*
>
> *[Ofcom workplan] "Evaluating the impact. We will monitor whether life is getting safer online." (2.22, p.16)*

We suggest that while proactive prevention is a laudable goal, the efficacy of automated tools and upload filters for preventing harm has not been established[2]. In particular, we raise a concern regarding the ongoing efforts to restrict access to encryption and anonymity technologies for both adults and children. There are essential contradictions in what policymakers desire from technology that cannot be reconciled.

We recommend Ofcom should not seek to extend the mandate of 'accredited technologies' but rather regulate for the desired outcomes.[3] Evaluating the outcomes, and "whether life is getting safer

[1] Ofcom's proposed Plan of Work 2026/27 themes pp35-37 https://www.Ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/consultation-plan-of-work-2026-27/main-documents/consultation-Ofcoms-proposed-plan-of-work-2026-27.pdf?v=408720

[2] Anderson, R. (2022). Chat control or child protection?. https://arxiv.org/pdf/2210.08958

[3] Anderson, R. and Gilbert, S. (2022) The Online Safety Bill Policy Brief, "Section 6. Recommendations". Bennett Institute for Public Policy Cambridge. https://www.bennettschool.cam.ac.uk/wp-content/uploads/2022/09/Policy-Brief-Online-Safety-Bill.pdf

online", therefore, must include a range of evidence including the unintended consequences for individuals and communities where access to information or secure services (such as encryption and VPNs)[4] is restricted in the name of "safety".

We recommend that Ofcom consult on the effectiveness and accuracy of its definition and methodology of what "safer online" means, how it is measured, and for whom, and to make this evaluation of impact prior to undertaking the assessment itself.

The communications technologies we use cannot simultaneously be secure in a global, networked Internet, and open to large-scale inspection by law enforcement and security services. There are direct conflicts with other government policy goals, for example, in the forthcoming *Cyber Security and Resilience Bill*[5]. Despite the apparent promise of technical 'fixes' to encryption that allow accountable law enforcement access, these technical changes create higher-order effects that fundamentally change the nature of security when incorporated into real systems. For example, attempts to create a Master Key that allows law enforcement access might appear to preserve the security of the system against non-law enforcement attackers, but in fact they simply make the load bearing element of the system the human administrator who controls access to the key (and is therefore subject to coercion and blackmail) rather than the mathematics of encryption and testable security designs.

We recommend that Ofcom engage in further consultation with technical expert groups, including FIPR, on the benefits and negative consequences to privacy, security, and civic rights, of potential designs, verify the design, to validate the implementation, and how to monitor the operation of technical solutions relating to upload filters, hash matching, measures on-device[6], and encryption workarounds, rather than leaving implementation and self-assessment to industry alone.

2.2 Demonstrating age checks are highly effective

Age assurance and age verification in the workplan raise questions of definition, engagement, and purposes, as well as suggesting potential gaps, which will need to be resolved to effectively cover emerging issues that will fall into the Ofcom remit.

2.2.1 Age checks: definition

> Work plan p.15 "*We [...] will take action where our evidence suggests that their solutions are not **sufficiently effective at determining whether a user is a child or adult**.*"[7]

[4] VPN companies 'open to meaningful dialogue' with UK government during children's online safety consultation (2026) Tech Radar https://www.techradar.com/vpn/vpn-privacy-security/vpn-companies-open-to-meaningful-dialogue-with-uk-government-during-childrens-online-safety-consultation

[5] Cyber Security and Resilience (Network and Information Systems) Bill (2026) https://bills.parliament.uk/bills/4035

[6] Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Callas, J., Diffie, W., Landau, S., Neumann, P. G., Rivest, R. L., Schiller, J. I., Schneier, B., Teague, V., & Troncoso, C. (2024). Bugs in our pockets: The risks of client-side scanning. *Journal of Cybersecurity*, *10*(1), tyad020. https://doi.org/10.1093/cybsec/tyad020

[7] [Ofcom Work Plan p.15] "we will continue to **work with** the adult industry to identify and address **non-compliance**. We will monitor the 100 biggest pornography sites to ensure that the most popular services continue to have **age assurance**

Work plan p.37 “Use of app stores **by children**.”[8] “**evaluate the use and effectiveness of age assurance by app store providers.”**

The definition of “highly effective” and “sufficiently effective” age assurance and age verification must be both technically informed and legally enforceable. The criteria[9] of “Technical accuracy”, “Robustness”, “Reliability” and “Fairness” fail to make any assessment of whether these make use “safer” for all users, and all children, not only the subset of children the age-gating measures may be put in place to protect.

Compliance by service providers with both the online safety and the data protection regime is mandatory and should not be considered a trade-off. However, the reality of determining safety and risk means that the scale of risk to all users must be assessed against the risk to some users. There are no clear criteria in the work plan or preceding publications to indicate whether this is assessed as a substantive or procedural obligation or whether a service is deemed “effective” because it has demonstrated compliance with the criteria of the task, or by assessing the outcome. That is, is age verification “effective” if a third party provider meets the ‘technically accurate’ claim in its lab, but over which it has no direct control when it is deployed by a user-to-user regulated service?[10] Does the assessment include the rate of effective avoidance by users?

There are serious technical challenges which pertain to any policy based around the existence of ‘highly effective’ age assurance. There is no single technology that can provide a definitive solution despite vendors’ claims. As a recent Georgetown report[11] argues, numerous technical approaches to implementation are possible. The privacy and security of the users of these systems are themselves matters of online harm and child safety. Further, methods to circumvent these systems abound - from stolen credit cards or shared devices to more technical methods of circumvention, such as AI generated documents and video.

The risks posed to young users by circumvention, the harms posed by incentivising them to use riskier unregulated sites, or by subjecting children’s use of the internet entirely to their parents’ scrutiny, will disproportionately accrue to the most vulnerable groups of young people.

---

and will take action where our evidence suggests that their solutions are not **sufficiently effective at determining whether a user is a child or adult**.”

[Ofcom Work Plan p.40] **Evaluation of Age Assurance measures** to understand the impact of Highly Effective Age Assurance (HEAA) on user visits to adult service as well as the extent of circumvention of HEAA (activities to be completed by December 2025 and; future evaluations to be scoped in Q1 and Q2 of 2026 (page 40))

[8] p.37 “Use of app stores by children. As required by the OSA, we will publish a report on the use of app stores by children by January 2027. This will assess the role app stores play in children encountering harmful content and **evaluate the use and effectiveness of age assurance by app store providers.** This will support the Secretary of State in determining whether app store providers should be brought into scope of the Act.”

[9] Quick guide to implementing highly effective age assurance, Ofcom [accessed on February 3, 2026]. https://www.Ofcom.org.uk/online-safety/illegal-and-harmful-content/age-assurance

[10] Ofcom Guidance on highly effective age assurance For Part 3 services (April 2025) https://www.Ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-age-assurance-and-childrens-access/part-3-guidance-on-highly-effective-age-assurance.pdf?v=395680

[11] Age Assurance Online: A Technical Assessment of Current Systems and their Limitations. (2026). *Knight-Georgetown Institute*. https://kgi.georgetown.edu/research-and-commentary/age-assurance-online/

Defining “effective” to suggest an obligation that user-to-user services adopt technical methods to clamp down on circumvention (such as restricting the use of VPNs) will in turn create new safety and security risks and needs a technically informed, evidence-based approach that is contextually appropriate to a variety of applications, whether in business, educational, gaming, or other settings.

We recommend that the workplan be expanded to include an independent audit of the efficacy assessment criteria and measures in practice, to demonstrate whether they are themselves effective, accurate, robust, reliable, and fair, and to measure and evaluate their impact. This should be carried out on a periodic basis to ensure understanding of the performance metrics remain reliable in step with changes in, and the emergence of new, technology.

2.2.2 Age checks: Ofcom engagement

The Ofcom workplan states **(p.15)** continued **engagement** is limited to ***work with*** only the adult industry, but the bigger and more important work relates to broader public policy.

We recommend urgent and ongoing engagement with the wider applications of age assurance and verification, broader consideration of other commercial environments, and consulting civil society expertise on its changing technical architecture, development and application. This must include questions of how compliance is determined in practice, enable the balancing act between highly effective age verification and minimising the unintended consequences.

2.2.3 Age checks: Ofcom aims

The **purposes** of demonstrating age checks are highly effective are stated as restricted to being for the purposes of ‘compliance’ and therefore enforcement **(p.15)** .

The scope of the workplan does not include age verification and age assurance in the context of the recent government consultation[12] that includes consideration of a social media “ban” for children, what age that might be applied to, shutdown laws, and content upload filters.

We recommend that Ofcom commission further research work and consultation on the technological evidence relating to approaches to age assurance and age verification prior to assessing efficacy. This should ensure consistent cross-sectoral standards fit for purpose in each context of use, not only in the context of adult services (as the work plan suggests), but for wider sectors of potential application and emerging UK legislative debate. FIPR is committed to the production of non-partisan expertise in technology and information policy and would welcome the opportunity to support Ofcom in this task.

[12] Government to drive action to improve children’s relationship with mobile phones and social media (2026) gov.uk https://www.gov.uk/government/news/government-to-drive-action-to-improve-childrens-relationship-with-mobile-phones-and-social-media

2.2.4 Age checks: What's missing

We recommend that Ofcom take forward a stream of research work exploring the role that platform technologies play in harm to children, building on the wealth of academic and practitioner expertise on these topics in the UK's regulatory context.

Although not easily separable, harms that arise from specific design affordances of a technology - such as how the user interface is designed - require different regulation from those which stem from core business models and misaligned incentives, or from the normative stance, moderation policies, or culture of a platform; or indeed from forms of organised harm which rely more on existing networks institutional power outside the platforms. This work could further critically monitor and evaluate international policy initiatives in this space and their early effects - and unintended consequences or harms to specific under-considered and marginalised groups, such as LGBT young people.

Beyond purely reactive enforcement, or policies focusing entirely on technological prevention through re-design of systems, there are a range of other models internationally which should be considered. For example, in the UK, the Childlight Global Safety Institute[13] represents a holistic, rights-centred approach to researching harms to children, in which technology is one component alongside a range of other social and institutional factors. In a European context, the direction of travel is towards decentralised distributed wallets for storing a range of credentials, including for age verification. However, serious consideration needs to be given to the wider unintended consequences of these kinds of approaches.

Age gating must not result in a 'data grab' by platforms for the collection of biometric data and demoting the content of users who do not want to provide this. If policy approaches remain narrowly technical and in the hands of the platforms to design, Ofcom's regulatory duty to balance and govern the power of major tech firms may come into conflict with its attempts to regulate harm. The ICO will be an important partner in taking this work forward.

3. International engagement and digital sovereignty

An increasingly urgent challenge in digital policy not considered by the Plan of Work is the role of cross-jurisdictional issues and also the international debates around 'digital sovereignty'. Significant work is underway at EU level to explore the decoupling of European nations' digital infrastructure from US-based providers, in favour of a 'Eurostack' of platforms and services. The rupture of the old rules-based order makes this an immediate concern. The UK position is different from that of the EU, in that it both relies deeply on American digital infrastructure for defence and security, and also provides substantial infrastructure for US global communications interception and surveillance. However, there is common agreement that neither Europe nor the UK can rely on the US as they used to.

Analysis of the impact of Ofcom's primary task of regulating online platforms that are almost exclusively based in other jurisdictions, many of them in the US, has not been done to date, and is crucial for the UK to carry out with urgency. There are therefore both jurisdictional and structural issues that will loom over Ofcom's work in the period covered by the workplan.

[13] Global Child Safety Institute (Edinburgh, UK) https://www.childlight.org/

We recommend that Ofcom develop a strand of exploratory work and a mapping exercise on digital sovereignty. This would cover the impacts that, for example, a move by EU nations to de-link from US infrastructure and platforms may have on UK users and policy, and potentially at policy options, scenario planning. We further suggest exploring the possible consequences for if in future the UK moves to decouple the consumer market from US digital infrastructure provision. This mapping exercise would help Ofcom management and staff understand the flashpoints and barriers that could be unintentionally created, especially with regard to critical public services, the NHS, and CNI as well as public communications infrastructure.

4. PSTN Switch-off

In relation to the upcoming switching-off of the Public Switched Telephone Network in 2027: The distinction between "number based" and "number independent" systems becomes blurred. There is an ongoing issue with the merging of SMS and RPC. The powers of Ofcom to regulate SMS are huge, including mandatory scanning for scams and fraud. This could clash with the importance of secure encryption in the core security design and creates the architecture and infrastructure for URL blocking.

We recommend that Ofcom should develop safeguards and policy statements to minimise the abuse of these systems to introduce rights restrictions, working with DSIT and a range of UK stakeholders.

5. Approach to AI

> *"AI continues to evolve at a rapid pace, and we are already seeing the next major advancement in consumer-facing capabilities, in the form of agentic AI." (p.21)*

There is increasing pressure for Ofcom to bring 'AI' into its regulatory scope. Internationally, there are many initiatives to regulate AI, and there are pitfalls in each of them. There are strong and potentially irreconcilable tensions between the US and the EU approaches. US Federal law now addresses AI, calling for [minimal] regulation. Where the EU moves to enforce compliance through their use of competition law, the US is using anti-trust law to shield its corporate interests. To get the desired benefits of AI for industry, the UK government and Ofcom, will need to navigate this complex field**.**

The statutory remit of Ofcom to regulate AI technologies is unclear. AI raises challenges in the online environment which are not within this remit, such as software tools which may be provided by a platform, and whose output may be communicated, but is not in itself, a communication. This has already been recognised by the Chair of the DSIT Select committee. An example would be Grok AI offered via the X platform.[14] A software tool, which can exist independently from a communications

[14] Because of the way the Act relates to chatbots, Ofcom is currently unable to investigate the creation of illegal images by the standalone Grok service. (Feb. 3, 2026) Ofcom update: Investigation into X, and scope of the OSA

service or online platform, would require a different form of regulation from the measures to address content posted online. Navigating this will be another crucial challenge for Ofcom to produce a workable way forward for all stakeholders.

A third challenge posed by AI in the field of communications relates to how Ofcom understands the unforeseen consequences of AI-based content moderation technologies. This relates to the core of Ofcom's work in relation to the Online Safety Act, and it may be the least appreciated element - until, that is, someone believes their content has been censored.

Ofcom is bound by the Act to operate measures drafted by a criminal lawyer in Whitehall, but is being constantly buffeted by the public's differing expectations. The challenge is to find a way to bridge that gap by developing a more transparent approach, and importantly, enforcing transparency on the AI systems of the public platforms.

Regulators including the DRCF (FCA, ICO, Ofcom and CMA) will come under increasing pressure to strengthen their activity and interventions in emerging 'hot topics' or new areas such as agentic AI and popular or media driven agendas.

We recommend that the scoping and horizon scanning of likely issues form a larger part of the workplan and include closer collaboration with leading academics and civil society. Given the impact from interventions for public trust, political backlash and international relations, this should include the establishment of a fast-track mechanism to inform and engage with the regulators for such matters, from informed bodies and individuals, assign responsible case owners within the most appropriate regulator(s) and timeframes for responses.

6. Conclusion

There is a danger that Ofcom, through its implementation of its role under the Online Safety Act, will become the de facto regulator for a wide range of technologies and policy areas beyond the brief of communications, including a range of AI technologies, pornography, CSAM, and political speech. We recommend that Ofcom work with policymakers on exploring a different regulatory structure to address these issues (such as stand-alone AI legislation) and push back against incorporating AI in their remit. This may mean it should ringfence its remit on the Online Safety Act and focus on the regulation of communications networks and platforms. There are, naturally, elements of this remit which include AI, such as content moderation systems, which use AI to identify and act on images and video, and monitor text-based content.

The international effects of Ofcom's intervention cannot be underestimated in relation to foreign policy, commerce and trade policy, science and technology policy, immigration policy, national security policy, anti-trust regulation, and highly political debates around consequences for the First Amendment.

We conclude by emphasising the importance of policymakers and regulators' engagement with technical stakeholders and expertise from outside the platform and 'big tech' industries, and of renewed consideration of the negative consequences of potential technical designs and restrictions. It is particularly important to consider the challenges - differing technical consequences, effects on rights,

https://www.Ofcom.org.uk/online-safety/illegal-and-harmful-content/investigation-into-x-and-scope-of-the-online-safety-act

and harms - posed for marginalised groups who, in the context of a global resurgence of far right politics, face both the most acute harms in online spaces and the most immediate potential for negative consequences from intensified digital surveillance. **We recommend that Ofcom commission further research work on currently proposed technological approaches to regulating platform-based public communication**. FIPR is committed to the production of non-partisan expertise in technology and information policy, and would be delighted to support Ofcom in this role, along with stakeholders from civil society.

7. About The Foundation for Information Policy Research (FIPR)

The Foundation for Information Policy Research (FIPR) is the leading academic think tank for Internet policy in Britain, established in 1998. It studies the interaction between IT, Government, business and civil society. It researches policy implications and alternatives, and promotes better understanding and dialogue between business, Government and NGOs across Europe.

To further these objectives, the foundation's current approach is to:

- monitor technological developments and policy initiatives in Government and business;
- identify how information technology issues affect business, freedom of speech, privacy, democratic governance, and the accountability and efficiency of public administration;
- commission and conduct research on relevant topics;
- disseminate and promote the findings of research;
- organise specialist seminars and conferences;
- work with Parliament, officials and others to improve the quality of Government policy making and legislation;
- use the news media to stimulate wider public debate about the policy implications of new and emerging developments in technology and public policy.

Policy is governed by an independent board of trustees in consultation with an expert advisory council.

The Foundation for Information Policy Research is a non-profit organisation registered in England under the Companies Act 1985 as a private company limited by guarantee (No. 3574631) with charitable objectives. The registered office address is '66 Huntingdon Road, Cambridge, CB3 0HH, UK'

FIPR was a founding member of European Digital Rights (EDRi), an association of civil and human rights organisations from across Europe, established in 2002, to defend human rights and freedoms in the digital environment. We maintain a close connection to emerging law and policy in the region, through the collective of 50+ NGOs, plus experts, advocates and academics across the EDRi network[15].

[15] European Digital Rights (EDRi) https://edri.org/