Department for
Science, Innovation
& Technology

Draft Statement of Strategic Priorities for Online Safety

Department for
Science, Innovation
& Technology

Draft Statement of Strategic Priorities for Online Safety

Presented to Parliament pursuant to Section 173 of the Online Safety Act 2023

May 2025

This publication is available at www.gov.uk/official-documents.

Any enquiries regarding this publication should be sent to us at osaimplementation@dsit.gov.uk

ISBN 978-1-5286-5464-7

E03303156 05/25

Printed on paper containing 40% recycled fibre content minimum

Printed in the UK by HH Associates Ltd. on behalf of the Controller of His Majesty's Stationery Office

Contents

Introduction

The online world provides many opportunities for society. It is a vibrant place full of ideas, information, and ways to connect with others, bridging distances between communities in every corner of our country and around the world.

The online world can also be used in ways that cause real harm to users and society. Too often, the internet has been a safe haven for illegal content and activity. For too long, children have been exposed to content that poses a real risk of harm to their psychological and physical wellbeing, and cases of people facing abuse online are far too high. Content capable of sowing division and inciting real-world violence such as hate speech or content inciting violence spreads too frequently with alarming reach and speed, spilling into our individual lives and onto our streets.

Tech companies benefitting from conducting their business in the UK must accept their responsibility to keep people safe on their platforms and foster a safer online world. Keeping people safe is the first duty of government and it should be the first duty online platforms have towards their users. The power platforms have to effect change is undeniable, but recognition of - and action on - their responsibilities has often been too slow and insufficient.

The Online Safety Act (the Act) puts a range of new duties on social media companies and search services, making them more responsible for users' safety on their platforms.

This Statement of Strategic Priorities (SSP) sets out the government's focus areas for online safety. The regulator, Ofcom, must have regard to these priorities as we continue to implement the Act. This statement has been developed with the input of those who have experienced the offline impacts of failures in online safety.

We must use all the tools we have available to deliver a safer online world. To do this, we will prioritise:

- implementing safety by design to stop more harm occurring in the first place
- increasing transparency and accountability of online platforms
- maintaining regulatory agility to keep pace with changing technology and behaviour
- building an inclusive and resilient online society of well-informed users
- supporting continued innovation in safety technologies

These priorities are, rightly, ambitious. Against a backdrop of rapid evolutions in online services and behaviour, these priorities will be backed by our commitment to continue iterating, innovating, and building on what works and fixing what doesn't. We will retain a relentless focus on these priorities, and we expect the same from Ofcom and the online services industry.

As well as asking the regulator to look at these strategic priorities, we remain committed to implementing the foundational protections of the Act.

This includes pursuing a reduction in illegal activity online. The Act requires online platforms to proactively identify and remove illegal content, including content related to terrorism, foreign interference, fraud, illegal abuse and threats, and stirring up hatred offences. Through the approaches in this statement, we will see a reduction in users' exposure to this content, whilst ensuring users' rights to privacy and freedom of expression are protected. We will also work to reduce instances of online users being exploited by fraudsters.

The Act ensures children have the strongest protections, and these strategic priorities will support the legal framework required to ensure these protections are implemented effectively and continue to improve. We will relentlessly pursue a reduction in children's exposure to harmful content.

As part of the government's specific mission to take back our streets we have committed to halve violence against women and girls over the next decade. To achieve this goal, it is vital we tackle the abuse faced by women and girls online. To tackle violence against women and girls, it is important that we develop an understanding of the experiences of different user groups, and how these manifest online. The Act, and the approaches in this statement, will seek to tackle illegal and misogynistic content to ensure increased safety online for women and girls.

Although we can and must work at pace, we do not expect to achieve all these outcomes immediately. We are committed to working on these issues alongside Ofcom, and to engaging stakeholders to continue to develop our approach in line with the government's mission commitments. We will continue to monitor progress and be evidence-driven.

Where it is clear some problems cannot be solved without new legislation, the government will consider this, but our goal is to be innovative and deliver maximum outcomes within the Act's existing provisions.

Government's Strategic Priorities for Online Safety

1. **Safety by design:** Embed safety by design to deliver safe online experiences for all users but especially children, tackle violence against women and girls, and work towards ensuring that there are no safe havens for illegal content and activity, including fraud, child sexual exploitation and abuse, and illegal disinformation

2. **Transparency and accountability:** Ensure industry transparency and accountability for delivering on online safety outcomes, driving increased trust in services and expanding the evidence-base to provide safer experiences for users

3. **Agile regulation:** Deliver an agile approach to regulation, ensuring the framework is robust in monitoring and tackling emerging harms - such as Artificial Intelligence (AI) generated content - and increases friction for technologies which enable online harm

4. **Inclusivity and resilience:** Create an inclusive, informed and vibrant digital society resilient to potential harms, including disinformation

5. **Technology and innovation:** Foster the innovation of online safety technologies to improve the safety of users and drive growth

Purpose for and basis of this statement

This statement sets out the government's strategic priorities in relation to online safety matters. The power for the government to designate this statement was introduced by the Online Safety Act 2023. This is the first time the government is exercising this power.

'Online safety matters' is defined by section 235 of the Online Safety Act 2023 and stipulates that priorities within this statement must be connected to Ofcom's online safety functions. As such, the statement focuses on priorities captured within the existing legal framework.

Ofcom must have regard to the statement when exercising its regulatory functions on online safety matters. Ofcom has a range of regulatory functions in scope of the statement including its functions established by the Online Safety Act 2023, such as those to enforce the regime or to develop regulatory products including Codes of Practice and guidance. A small number of its general regulatory functions under the Communications Act 2003 are also in scope such as Ofcom's duty to promote media literacy. Further detail on the legislative framework for the SSP is set out below.

The statement establishes government's priorities for the online safety agenda. We recognise that Ofcom's functions in relation to some of the priorities set out within this statement are more limited. As the independent regulator for the online safety regime, it will be for Ofcom to determine how it can best respond to the priorities within this statement. However, the government is clear that alongside consideration of these priorities Ofcom should continue to deliver other workstreams as planned. If Ofcom is unable to use regulatory options to contribute to achieving the strategic priorities set out in this SSP due to the existing statutory framework, the government will consider bringing forward legislation to allow it to do so.

The legislative framework

The Online Safety Act 2023 sets out the legislative framework for the Statement of Strategic Priorities.

Under section 172, the Secretary of State may designate a statement that sets out the government's strategic priorities relating to online safety matters. The statement cannot be amended within five years unless there is a general election or a significant change in government policy, or the Secretary of State considers that the statement, or part of it, conflicts with Ofcom's general duties. Section 172 also provides that the statement may set out particular outcomes identified with a view to achieving the strategic priorities.

Under section 173, before designating a statement, the Secretary of State must consult Ofcom and such other persons as they consider appropriate on a draft of the statement, allowing at least 40 days for a response. The Secretary of State must then make any changes to the draft that appear to them to be necessary in view of responses to the consultation and lay the draft before Parliament for a 40-day period, excluding Parliamentary recesses. The Secretary of State may then designate the statement unless either House of Parliament resolves not to approve the draft within that period.

Under section 92, Ofcom must then have regard to the statement when exercising relevant functions. Ofcom must explain what it proposes to do in consequence of the statement within 40 days of the designation of the statement or such longer period as the Secretary of State may allow. Ofcom must also, as soon as practicable after a period of 12 months from the designation of the statement and after every subsequent period of 12 months, publish a review of what it has done in the period in question in consequence of the statement.

Statement of Strategic Priorities

1. Safety by design

When we discuss safety by design, we mean that regulated providers should look at all areas of their services and business models, including algorithms and functionalities, when considering how to protect all users online. They should focus not only on managing risks but embedding safety outcomes throughout the design and development of new features and functionalities, and consider how to make existing features safer. The government believes the goal should be to prevent harm from occurring in the first place, wherever possible. While this is clearly a material challenge, Ofcom has significant powers at its disposal - including information gathering, audit, enforcement and penalty powers - to ensure providers comply with their statutory duties to protect users online.

The government wants all users to be able to enjoy the benefits of safe online spaces. The expectation cannot fall on users to take precautionary steps to avoid illegal content online. Children should also not be responsible for protecting themselves from harmful content. We want to see services that are safe by design, where features are chosen and designed to limit the risk of harm to users. This should be a basic principle for operating in the UK market.

Content promoting acts of serious violence, peddling hatred and inciting acts of suicide and self-harm are far too easily accessible by users who wish to be or should be protected from such content, especially children. There have been too many tragic cases which illustrate the impact this has on young people's lives.

While protections should be strongest for our children, all users should have better protections online and feel supported to make choices about what they see. We know that 93% of adults are "very concerned" about harms they might experience online, including hateful, offensive or discriminatory content (55%), content promoting self-harm (62%) and misogynistic content (45%).[1] The government is particularly concerned about the amount of abuse women and girls receive online, with Ofcom's annual Online Nation report finding that women are more likely to encounter misogynistic content or content relating to negative body image and are more likely to be negatively affected by harmful content they encounter.[2] The government is also concerned that, whilst the share of fraud committed online is falling in England and Wales, it is still too high. In the absence of government intervention, we estimate the cost of fraud originating online to be £18.9bn over 2024-2033 arising from 1.6 million offences.[3]

[1] Ofcom, Online Experience Tracker, Wave 6, 2024

[2] https://www.ofcom.org.uk/media-use-and-attitudes/ online-habits/ online-nation/

[3] Online Safety Act Enactment Impact Assessment 2024, Table 38- Fraud cost

Following the Southport tragedy in July 2024, we also saw how the proliferation of hateful content online fuelled violence and civil unrest across the UK. We saw violent attacks on temporary accommodation for asylum seekers, mosques, businesses, law enforcement and individuals. The rampant spread of misleading information and incitement to violent disorder legitimised the violence and escalated it, spreading fear amongst the public. It is essential that we learn from these events and hold platforms to account for their part in securing the UK online information environment and safeguarding the UK from future crises.

Safety by design approaches will improve the online experience for all users. However, there is also specific, targeted action that we believe should be considered in tackling specific harms and to protect the most vulnerable users. The government's strategic priorities for embedding safety by design are set out below.

1.1 Developing a strong evidence-base to support children to have safe, age- appropriate experiences online

The government is clear that it expects the strongest protections on services to be provided for children. It is crucial that we continue to build evidence on the impact, prevalence and types of content online that is harmful to children at different ages and keep pace with new trends in how children interact with harmful content. Engaging with children is a key aspect of this; research should amplify children's voices in the policymaking process and strengthen the evidence-base.

In particular, the government would like to see a focus on building upon the evidence-base around age-appropriate experiences to work towards more detailed recommendations for companies on how to protect children in different age groups.

A robust and comprehensive evidence-base on safe service design will be integral to the development of codes of practice, and Ofcom should use all of its levers and powers to ensure that the unsafe design of services is identified and tackled through its codes. Ofcom should continue to research new methods for keeping children safe on services and use these findings to inform parents, carers and the public about how to protect children online. The child safety codes should be iterated as new effective measures for protecting children are developed.

1.2 Ensuring companies are effectively deploying age assurance technology to protect children from harm online and investing in technological developments

Services should take advantage of the technologies that are already available to identify child users and ensure that they cannot access harmful content on their services - this includes both age estimation and age verification technology. Age assurance should be deployed consistently, effectively and fairly to users from all backgrounds and age ranges.

Crucially, the Act requires a wide range of services to deploy highly effective age assurance to protect children from extremely harmful content, including pornography and content that encourages, promotes or provides instructions for suicide, self-harm or eating disorders. Ofcom's regulatory approach should promote the continuing development of age assurance technologies to further improve child safety outcomes, particularly with regard to identifying children of different age groups to deliver age-appropriate online services, and create an environment where platforms deploy these technologies safely.

1.3 Deploying effective and accessible additional protections for adult users, particularly vulnerable users

Whilst the most robust protections in the Act are for children, the government recognises some adult users would benefit from access to additional protections from content which does not meet the bar for illegality but could still be harmful. All users, particularly those who are vulnerable, should feel supported to make choices about what they see online. Companies offering online services have a clear responsibility to keep all their users safe from harm.

Category 1 services [4]should be designed to enable adults to make informed decisions about their online experience. Adult users should have effective and easy access to tools which they can choose to apply to reduce the likelihood that they will encounter certain types of content, this includes suicide and self-harm content which does not reach the criminal threshold. This will provide adult users with greater control over their online experiences.

They should be able to verify their identity and have access to tools which will help stop anonymous trolls from contacting them. We know that users are able to access harmful content via search engines, and so where it is proportionate to do so, these services should offer user support measures, which could include signposting users towards sources of support. Companies should have effective, accessible mechanisms in place for adult users to be able to report abuse and receive an appropriate response from the platform. This will make sure platforms are transparent and accountable to their users about what they will and won't allow on their services through consistent enforcement of their terms of service.

A particular area of focus for the government is misinformation and disinformation presenting a risk to national security or public safety that can be encountered by users online. Platforms should have robust policies and tools in place to minimise this content where it relates to their duties under the Act. Countering misinformation and disinformation is challenging for services, given the need to preserve legitimate debate and free speech online. However, the growing presence of disinformation poses a unique threat to our democratic processes and to societal cohesion in the

[4] Category 1 services are user-to-user services over a designated threshold, Category 2A services are major search services and Category 2B services are other categorised user-to-user services.

UK and must be robustly countered. Services should also remain live to emerging information threats, with the flexibility to quickly and robustly respond, and minimise the damaging effects on users, particularly vulnerable groups.

1.4 Using risk and evidence-based approaches to work towards ensuring there are no safe havens online for illegal content and activity

Providers must use risk and evidence-based approaches to ensure there is no room for illegal content and activity on their platforms. We expect providers to understand the level of risk of their service being used to facilitate illegal activity, including potentially during periods of crisis, and to embed safety by design principles to mitigate these risks. This should include steps in areas such as the design of a service, including algorithms and functionalities, policies on terms of use and, where proportionate, deploying technology to improve the scale and effectiveness of content moderation, considering factors including providers' capacity and users' freedom of expression and privacy rights.

We expect this to result in a material reduction in instances of **UK** users encountering illegal content through online services, and of online platforms being used to facilitate priority offences.

The government is also clear that it expects platforms to take proactive steps to reduce the risks their services are used to carry out the most harmful illegal activity. This includes:

- terrorism
- child sexual abuse and exploitation
- illegal suicide and self-harm content
- illegal activity which disproportionality affects women and girls, such as harassment, sexual exploitation, stalking, controlling or coercive behaviour and extreme pornography and intimate image abuse
- illegal disinformation and hate which incites violence towards specific individuals or groups, leading to societal fragmentation and disorder
- UK-linked content designed to encourage or facilitate organised immigration crime by criminal groups, as well as illegal sales of weapons and drugs
- illegal foreign interference, including state-sponsored disinformation, aimed at subverting the UK's democratic, political and legal processes
- illegal fraud; and
- other priority offences

In addition, the government is concerned that the advent of AI tools may facilitate coordinated inauthentic behaviour at scale. Particularly if used in tandem with established tactics to manipulate the information environment, there is an increased potential for foreign interference seeking to undermine the UK's core values and processes. It is vital that Ofcom's illegal content Code of Practice, which includes guidance on how platforms should mitigate and tackle illegal foreign interference, is fit for purpose if we are to adequately respond to this emerging threat.,_

The government set out its commitment to tackle fraud in its manifesto. Through the implementation of safety by design measures, including additional measures for Category 1 and 2A services to tackle fraudulent paid-for advertising, we expect over time to see a material reduction in online fraudulent content and activity on in scope services, resulting in fewer users being victims of fraud and scams, such as deepfake enabled scams.

The government is also clear that terrorism content and child sexual abuse material must be tackled in our online environments. To achieve this, we expect Ofcom to use powers at its disposal to oversee a reduction in such content.

2. Transparency and accountability

UK users are concerned about what they see and experience on the internet. 32% of 13-17-year-olds encountered Primary Priority Content such as pornography, suicide or self-harm content in a four-week period in 2024 and 30% of adults encountered content that made them feel "uncomfortable, upset or negative" in the same period.[5] A national investigation found that suicide-related internet use (including searching for information about suicide methods or posting messages with suicidal content) was reported in around 80 suicides by young people each year.[6]

Regulated services have a significant impact on both individual users and society more broadly. Greater transparency makes it easier for users and the regulator to hold services to account for this impact, pressing services to take responsibility and keeping users and wider society safe.

A transparent sector will allow us to identify both wrongdoing and best practice. Identifying where things are going wrong, through transparency reporting, research and effective user redress mechanisms, allows corrective action to be taken by services and the regulator to avoid repetitive wrongdoing. Identifying where services are fulfilling their safety duties will allow others to learn from their best practice.

Being transparent about where harms are occurring also enables users to choose which services to use. Users should be empowered to make informed choices about where they want to spend their time online, and users exercising this choice can also incentivise companies to make safety a core part of their business.

Together, transparency and accountability will improve trust in platforms, helping everyone to enjoy the services they offer. The government's strategic priorities in relation to transparency and accountability are set out below.

2.1 Improve transparency to increase understanding of the harms occurring on platforms, why they are occurring and the best way to tackle them

We cannot effectively tackle online harms if we do not know what harms are occurring, where they are occurring, how frequently, and to whom.

For example, it is not clear how platforms' algorithms work, how that impacts on the dissemination of harmful content or its prioritisation over other content and how this issue varies between platforms, as well as the incentives which drive platforms' decision-making about the design of these algorithms. More research is needed to understand how this content is disseminated throughout the population, including how this varies between different platforms and users. This includes the use of automated systems (artificial intelligence/machine learning) to recommend content to users. Algorithmic transparency may also be an area of interest for other regulators,

[5] Figures drawn from the Ofcom Online Experiences Tracker (Wave 6), 2024

[6] s..u.LcicleJuc..hi.L�o__ung_p_e_QpJ.e...l-!atLonaLC_Qnfi.ctentiaLln__quilyjntQ_fau_clcte_and.J:iomiclde_by_Ee_QP.l.e. with MentalIllness (NCISH). Manchester: University of Manchester, 2017.

such as the Information Commissioner and the Digital Markets Unit, and we would encourage regulatory coordination in any areas where interests overlap.

Alongside Ofcom's evidence-gathering activities, such as conducting and commissioning research, one important tool for increasing our online harms evidence base is the Act's transparency reporting regime. The government wants to see a culture of candour created through Ofcom's transparency reporting regime, where the regulator and platforms work together to expose practices that create the greatest risks to users and address the systemic issues they uncover.

The transparency reporting regime should also highlight best practice and provide clear examples of what platforms can do to keep their users safe. We encourage all platforms to offer transparency around all in-scope types of harmful content that they have assessed could be encountered by users or facilitated via their services, and what they are doing to address these. The government is keen to see services embed examples of industry best practice that provide continuous improvements to user safety on their services while respecting human rights.

To ensure that this information can be meaningfully used by the public, transparency reports should be clear, easy to use and accessible. At the same time, transparency reports should also have sufficient detail and depth to ensure that they can be used by researchers to improve understanding of online harms and understand why they are occurring, and by law enforcement to keep the public safe. In addition to Ofcom's mechanisms to increase our knowledge of online harms, independent researchers should feel empowered to contribute to this evidence base. The government wants researchers to have access to the data they need to continue to develop our knowledge on both harms and solutions. The Data (Use and Access) Bill contains provisions which, subject to completing parliamentary passage, will complement the transparency reporting regime by giving the Secretary of State the power to introduce a new regime for data access, ensuring researchers can access the vital, in-depth data they need from providers to undertake analysis of online safety risks to UK users.

The government also wants to see forward-looking, impact-focused advice from the Advisory Committee on Disinformation and Misinformation that Ofcom are establishing. The expert, cross-sector advice generated by this committee will be crucial for growing understanding of how misinformation and disinformation can be tackled online.

Over time, these measures will develop our evidence-base concerning the harms occurring online, so we can more effectively compel platforms to create environments where everyone is protected and support users to make more informed choices about which platforms they want to use.

2.2 Parents and carers are treated with respect when requesting information from services following the death of a child, and, through Ofcom, coroners have access to data to understand how online activity may have contributed to the death of a child

It is crucial that we support those families who have endured unimaginable losses and ensure that the right measures are in place to get parents the answers they deserve after a tragedy.

Parents and carers should not have to fight to make contact with platforms following the death of a child, and we expect categorised services to respond to parents and carers' requests in a humane and transparent way. They should have systems to make information requests which are easy to find, easy to use and which keep parents updated as their request progresses.

Ofcom has the powers to request relevant information from companies required for investigations into the death of a child, and to provide this information to coroners. These powers should be used to provide much needed answers to coroners in the most tragic of circumstances so that bereaved families can be confident their inquests will get to the heart of what happened. To build on this, the new Data (Use and Access) Bill will establish a further data preservation notice process. This would require Ofcom, on notification from a coroner, to issue a notice to specified services requiring them to retain relevant data they may have on a child which could later be required in an inquest. Additionally, government is committed to continue working with Ofcom, law enforcement and coroners to ensure these powers are effective in each relevant circumstance.

2.3 Users are clear what is allowed on services through providers' Terms of Service, and these are applied consistently

The government expects all providers of regulated user-to-user services to have clear and accessible Terms of Service provisions about how they fulfil their illegal content, child safety and complaint reporting duties and apply them consistently.

The government expects Category 1 services to have clear and accessible Terms of Service that state what kinds of legal content for adults they do not accept on their platforms, and to write in sufficient detail what offences will result in a user being banned or suspended from their platform. Ofcom should hold services accountable to ensure that they apply these terms consistently, fulfilling their promise to users that if content is in breach of their terms then it must be removed.

Clear and transparent Terms of Service will enable adult users to understand what kind of legal content a service will not allow and help them to make decisions on engagement off the back of this. It is vital that all UK users - including children - are made aware of and can understand the Terms of Service. Special consideration for accessibility should be given to vulnerable individuals or those with additional needs.

Clear Terms of Service will also mean that all users can hold services accountable through user reporting and redress mechanisms if they don't uphold these terms.

Effective reporting and redress mechanisms will also be important to enable users to raise concerns about companies' enforcement of their Terms of Service if they feel that companies are not fulfilling their duties.

2.4 Platforms are accountable to users, increasing the incentives on providers to keep their users safe and benefit wider society by fostering a greater level of trust, safety and transparency

The government is clear that platforms must take the action needed to deliver user safety on their platforms, ensuring they are accountable to their users and to society more widely.

As noted in Ofcom's evidence gathering on illegal harms[7], providing simple, easy to understand terms and conditions, in tandem with a clearly sign-posted and accessible complaints system will benefit both users and the service providers.

Improving the user complaint experience and ensuring users are confident in its use will mean that service providers can appeal to a public who are more aware of the importance of user empowerment and redress in choosing which platforms they engage with.

Adults should also be able to make informed decisions about what services to engage with. It is therefore important to focus on the inclusiveness and accessibility of complaints and redress systems. Currently, these systems can be difficult to navigate, creating barriers that exclude large sections of the population. It is crucial that these processes are clear, accessible, and open to all and that everyone can seek redress effectively and receive an appropriate response from the platform. This includes in relation to journalism, content of democratic importance and also news publishers' content that has been shared on in-scope services. This also includes designing these mechanisms with the experience of all users, including survivors, in mind, meaning that all users will be better able to report abuse, helping survivors to know where to go for that help, including when the abuse is from someone known to them. Ofcom have been empowered by the Act to provide robust oversight of providers' performance in relation to their own terms and conditions. The Act provides Ofcom with robust information gathering powers and a transparency reporting regime allowing them to achieve a strong level of oversight. The Act also mandates that Ofcom is required to produce a report on the efficacy of the Act's user redress provisions within two years of section 160 coming into force, with the option for the Secretary of State to introduce an out-of-court dispute resolution system if deemed necessary. The government would recommend that Ofcom analyses user complaints to identify trends that may require further systemic-level action, such as additional research, engagement with services, or consumer campaigns to assess whether regulated services are appropriately protecting their users. This can be

[7] https:t/www.ofcom.org.uk.lonline-satety/itlegal-and-harmful-content/protecting-peopte-trom-illegat-content-online/

complemented by wider research into public satisfaction with providers' safety measures and complaint processes.

3. Agile regulation

The online environment is continuously and rapidly changing. It is essential that regulation keeps pace with changes that can impact online safety.

There are several ways in which changes in the online environment can impact user safety. While new technology can be a key tool for improving online safety, technologies can also emerge which have different risk profiles that need to be accounted for and these need new safety measures to combat harms.

In addition, existing technologies can be used in different ways as online culture and behaviour changes, and as the service providers themselves change their offering. Such changes can enable people to avoid safety measures by using existing technologies to enter less well-regulated spaces.

The Act has been designed to be broad and future-proofed so that it can take account of such changes where possible. To do this effectively it is important that regulation is agile. Ofcom may find significant benefits in designing a forward-looking approach to regulation that quickly mitigates significant risks that emerge. This includes where individuals are carrying out illegal and harmful activity in new ways, via new online technologies which enable user-to-user interactions. The government's strategic priorities in relation to agile regulation are set out below.

3.1 Changes in the use of technology that enable online harm are monitored, risk assessed and where appropriate mitigated against

The first duty of government is to keep citizens safe and the country secure. The internet, as vital as it is to our society, is increasingly posing challenges to the safety of our citizens, especially the most vulnerable. The Act provides the tools for government to mitigate these risks and Ofcom has a vital role to play in delivering this.

However, this important mission has significant challenges. Technological innovations, which are developed and deployed at pace, potentially pose a risk to the efficacy of the Act.

The regulatory framework has been designed to be future-proof. The government would encourage Ofcom to utilise the full provisions of the Act to mitigate the use of existing/new technologies for harmful purposes, monitoring and guiding the platforms' own risk assessments and reinforcing the duty of platforms to put in place measures to ensure that new technologies are safe for users. Ofcom will further benefit from ensuring that the codes of practice and guidance, which set out how services can assess risks and comply with their online safety duties, reflect best practice on how providers can assess and mitigate new and emerging threats so that platforms can benefit from understanding how they can comply with these duties.

It is important that, in tandem with a risk-based approach by service providers, Ofcom can monitor the public's awareness and use of new technologies, especially by children, and the pathways that can lead users to unsafe spaces on the internet.

Lastly, in making the best use of regulatory tools, it is important that this is done in an iterative and agile way. This will ensure that relevant products are updated as quickly as possible and there is no gap in regulation. Given the pace of technological change, and the resulting risks to user safety, it is important that regulation does not fall behind. As such, Ofcom should be proactive in consulting on, and using the agility provided to it by the Act, to make relevant changes to guidance and codes.

3.2 Threats from AI-generated content and activity are effectively mitigated

One specific example of emerging technology is AI. AI tools and technologies are evolving rapidly. This is likely to create new challenges to society's resilience, as well as the ability of internet users to freely express themselves online and to seek out reliable information. At the same time, AI also creates the potential for technical tools that can improve resilience, by supporting services and users in controlling the kind of content they interact with.

Building on the work it set out in its *Strategic Approach to AI 2024/25,*[8] Ofcom should engage with DSIT on an annual basis, in April of each year, on whether changes in the AI landscape warrant the publication of an updated Strategic Approach to AI. Ofcom should identify and mitigate risks to users emerging from the sharing of AI-generated content on regulated services, and the deployment of AI by regulated services on their platforms, such as AI-driven content recommendation systems and embedded AI tools for users.

Ofcom and the government would mutually benefit from continuing to engage on emerging AI risks and technologies to ensure new risks are addressed. The government would also recommend that Ofcom works collaboratively with other regulators with the aim of aligning approaches to risks that cut across regulatory remits.

To support this work, the government would support Ofcom continuing to build its evidence-base on emerging AI risks, particularly as risks relate to children, and to explore the impact of generative AI on the creation and proliferation of harmful and illegal content. The government would welcome Ofcom continuing to analyse the benefits and limitations of specific measures that actors across the technology supply chain can take to respond to deepfakes, building on its *Deepfake Defences* and *Red-Teaming for GenAI Harms* discussion papers.[9]

[8] Ofcom's strategic approach to AI 2024/25 (March 2024), https://www.ofcom.org.uk/_data/assets/pdf_file/0021/281622/Ofcoms-strategic-approach-to-AI.pdf

[9] 'Deepfake Defences - Mitigating the harms of deceptive deepfakes', Ofcom, https://www.ofcom.org.uk/siteassets/resources/documents/consultations/discussion-

3.3 International cooperation should enable new ideas to tackle online safety to be shared, building a global consensus on online safety

Given the cross-border nature of the internet, we recognise the need for the government and Ofcom to work closely with and learn from international partners to enhance regulatory coordination and coherence. The UK must continue to build support for risk-based approaches to online safety which uphold our fundamental freedoms and hold tech companies to account across jurisdictions. The government will ensure the UK is at the forefront of work to develop shared principles and common standards and encourage innovation in the development and deployment of safety technologies. This will be more important as we navigate the impact of new and emerging technologies.

We will continue to work with Ofcom on initiatives to advance international collaboration on online safety, including through multilateral fora such as the OECD. We have given Ofcom powers to share information to support the work of other online safety regulators through section 114 of the Act, and we expect Ofcom to use its expertise and experience to promote increased coordination internationally. We strongly welcome Ofcom's role in driving forward the Global Online Safety Regulators Network to facilitate cooperation amongst regulatory bodies.

3.4 Small but risky services are regulated effectively

Small but risky services, including pro-suicide sites, are known to not only share information about how to die by suicide, but also enable active encouragement of self-harm/suicide. Hate forums are another type of small but risky service and are known to exist purely to fuel hate and division, often spreading illegal misinformation and disturbing racist and misogynistic content. Although the government is concerned about such content on services of all sizes, these particular types of services do not have their users' best interests at heart and can be exceptionally dangerous. Under the Act, all user-to-user services, including small but risky services, will be required to remove illegal content on their service. In particular, they must put systems and processes in place which are designed to proactively prevent users from seeing illegal suicide content. They also need to put systems in place to proactively manage the risk of users being harmed by other content whose publication amounts to a priority offence, such as public order offences, harassment or stalking, including fear or provocation of violence. Where relevant, such sites must also keep children safe from content which does not meet the criminal threshold but is nonetheless harmful to them. This includes preventing children from seeing harmful legal self-harm and suicide content. These are crucial duties which apply to all in-scope user-to-user services and apply irrespective of whether a service is categorised or not.

papers/deepfake-defences/deeptake-defences.pdf?v=37075A;' Red Teaming for GenAI Harms - Revealing the Risks and Rewards for Online Safety', Ofcom, hnps://www.ot.c_cun._o_rg..uklsite_as_s_etsLJ:e_s_o_ute..e_sldo_c.uments/c.0nsuttatLonsldis_c_u.s_siokp_ap_e.rsLrad:.teaming/red-teaming-for-gen-ai-harms.pdf?v=370762.

The government appreciates that Ofcom has set out to government its bespoke approach to tackling small but risky services. The government notes Ofcom's approach to tackling such services under its current video sharing platforms regime and that formal enforcement action was taken where improvements did not happen.[10] The government would like to see Ofcom keep this approach under continual review and to keep abreast of new and emerging small but risky services, which are posing harm to users online.

As the online safety regulator, we expect Ofcom to continue focusing its efforts on safety improvements among services that pose the highest risk of harm to users, including small but risky services. The government expects to see enforcement action taken against small but risky services which do not comply.

All search services in scope of the Act have duties to minimise the presentation of search results which include or lead directly to illegal content or content that is harmful to children. This should lead to a significant reduction in these services being accessible via search results.

[10] 'Letter from Dame Melanie Dawes to the Secretary of State', Ofcom, 2024, https://www.ofcom.org.uk/about-ofcom/what-we-do/public-correspondence/

4. Inclusivity and resilience

The government wants the internet to be a place of respectful engagement, diverse voices and responsible content creation. However, creating a safer internet does not come at the expense of a dynamic and competitive technology sector, and there are strong protections throughout the Online Safety Act to safeguard freedom of expression online. Being online offers a wealth of opportunities to improve people's lives by allowing them to connect with loved ones, learn something new and benefit from digital services to make their lives easier.

Alongside the potential for positive transformation, the advancement of digital technologies has brought about risks to the way people engage with the information environment. With so much information available, it is concerning that more than a third of UK adults (16+) who go online are unaware that content might be false or biased, according to Ofcom research.[11]

Without the skills to navigate the digital world, users are more exposed to harmful online content and ultimately can disengage from society, with serious and enduring consequences for communities and democracy. We also know that issues in our information environment can pose immediate, acute risks to public safety offline, such as the role that social media played in the public disorder in Summer 2024.

Media literacy can help tackle a wide variety of online safety issues for internet users of all ages. While precise definitions vary, the term refers to the broad range of skills and knowledge that internet users need to make safe and informed decisions online. This includes understanding that online actions have offline consequences, being able to engage critically with online information, and being able to contribute to a respectful online environment.

Platforms clearly have an important role in implementing robust online safety regimes. Complementary to this, Ofcom has a statutory duty to promote media literacy, which includes helping users understand the nature and impact of harmful content and online behaviour, especially where this disproportionately affects certain groups, such as women and girls.

Ofcom is required to publish a media literacy strategy at least once every three years. Their first strategy, 'A Positive Vision for Media Literacy', outlines three key areas of focus until 2027. Ofcom will conduct research and evaluation, to increase people's understanding of media literacy and 'what works' in interventions. They also plan to engage with platforms and broadcasters to enhance the media literacy support available to users. The strategy also includes commissioning initiatives and building relationships with key stakeholders, to ensure more people have access to high quality media literacy support and that media literacy is a greater priority for a broader range of organisations and sectors.

[11] https://www.ofcom.org.uk/media-use-and-attitudes/media-habits-adults/ adults-media-use-and-attitudes

The government welcomed the publication of Ofcom's strategy and looks forward to collaborating with Ofcom on its implementation. DSIT will play a crucial role in coordinating media literacy efforts between Ofcom and other government departments. For example, DSIT officials collaborate with the Department for Education to help ensure that media literacy is a key component of the educational curriculum.

Ofcom also has new transparency-reporting and information-gathering powers, which allow the regulator to request information from platforms on how they are tackling misinformation and disinformation within the scope of the Act. The Act also places risk assessment duties on in-scope companies, which require them to consider how they can use media literacy measures to mitigate the risks from harmful content on their platforms.

To strengthen protections for women and girls, Ofcom have published draft guidance that summarises, in one clear place, the measures that can be taken to tackle the abuse that women and girls disproportionately face online. The government recognises that this online abuse can manifest into violence offline. This guidance is a bold and ambitious step in encouraging services to take up innovative best practices and to address violence against women and girls holistically. This guidance will ensure that it is easy for platforms to implement holistic and effective protections for women and girls across their various duties.

The Independent Pornography Review was published on 27 February 2025. The report was clear that pornography is one part of a wider online environment and the findings about potential links to violence against women and girls will be considered by the government as part of its determination to tackle such violence. Action is required by multiple departments to consider the Review's recommendations in their areas and take them forward if appropriate. In the Written Ministerial Statement published alongside the final report, the government noted that graphic strangulation pornography is illegal, but is not always being treated as such. The government will take action to ensure pornography platforms, law enforcement and prosecutors are taking all necessary steps to tackle this.

The government further recognises the challenge posed to the resilience of individuals and society as a whole by the increased availability of AI tools that are capable of generating realistic content. The government therefore welcomes Ofcom's research into these risks and possible interventions, especially ways to support resilience by providing more transparency to users on the content that they are seeing. The government's strategic priorities in relation to an inclusive and resilient society are set out below.

4.1 Users who are aware of and resilient to mis- and disinformation

This government is committed to promoting the public's awareness of and resilience to misinformation and disinformation online. This includes developing public consideration of the reliability, accuracy and authenticity of content. Media literacy initiatives are therefore the cornerstones of conscious consumption of information online and should be used to pre-emptively build the public's resilience to information threats.

As part of a multi-faceted approach to tackling information threats, the government wants Ofcom, in their role as the regulator, to coordinate with tech companies, civil society organisations and education providers to deliver interventions that help the public identify and protect against mis- and disinformation. We expect the Advisory Committee on Disinformation and Misinformation, which Ofcom is establishing, will play a role in this by bringing together sector experts to advise Ofcom on appropriate responses to misinformation and disinformation. These interventions should be directed where the need is greatest, such as particular at-risk groups or geographic areas where they will have the most impact.

Building evidence on effective media literacy interventions is crucial. We value Ofcom's expert evaluation guidance, which helps organisations of all sizes to assess their initiatives. Ofcom is in a unique position to share these insights with the wider sector, leading efforts to improve best practices and guide future interventions.

It is important to note that the nature of disinformation is constantly evolving, both as a result of geopolitical dynamics worldwide, and in terms of how this content is created and shared. In particular, the increased use of AI tools creates a range of new risks and opportunities. Within this context, we expect Ofcom to undertake research and build evidence to keep up with new and advancing issues, especially to understand the impact on user behaviour and trust.

4.2 Widespread adoption of best practice principles for literacy by design provides users with the tools to navigate their online environments

The government welcomes the goals set out in Ofcom's three-year Media Literacy Strategy, particularly the proposed activities to engage platforms on best practice and ensure this goes further than online safety duties. The government encourages platforms to work closely with Ofcom in implementing this best practice.

Building on their 'Best Practice Design Principles for Media Literacy', Ofcom should continue to develop a clear framework for good platform design that aims to strengthen media literacy capabilities. This should consider where innovative approaches and features can support users to make more informed decisions online. The government would like to see commitment to these best practice principles and demonstrations of leadership from online services in this matter.

Furthermore, it is important that systems are established for monitoring, evaluating and improving these best practice principles in a transparent way.

4.3 Parents, carers and children understand risks and are supported to stay safe against online harm

The government's aim is to ensure that parents and carers are supported and have the necessary information to understand the online harms landscape to protect children's welfare.

Children are becoming increasingly present online, and this only increases the importance of equipping children with strong media literacy skills to help them make informed and safe choices online. This is underlined by the fact that a third of 8-17-year-olds report having seen something worrying online in the past 12 months.[12]

The government has announced an independent review of curriculum and assessment. The review will be rigorously evidenced and data-driven and will look closely at the barriers in the existing system which hold children back from the opportunities and life chances they deserve. The review will consider the key digital skills needed for future life and the critical thinking skills needed to ensure children are resilient to misinformation and extremist content online.

Ofcom should complement these efforts by continuing to expand and leverage a diverse network of organisations outside of formal education that reach parents, children and vulnerable families, directly and indirectly, to make media literacy and online safety a priority.

4.4 Young people feel included in the policy making process shaping their digital experiences online

Ofcom's codes of practice are designed to protect users, particularly children, and it is important that those users are engaged in the development of the codes. Ofcom has rightly engaged with thousands of users through its research and consultations while implementing the Act. It is important that, as implementation continues, Ofcom commits to further engagement with the users which the Act seeks to protect, including parents and children. Children should have a voice in the policy making process, and the participation of children and other users in the development of Ofcom's codes is an important tool in the production of effective protections for users.

4.5 Risks to trust in online information due to AI-generated content are effectively mitigated

Motivated or sophisticated actors, with good intentions or otherwise, can create AI content that is hard to distinguish from human-generated content - often creating false content and spreading mis- and dis- information online.

The government is committed to protecting individual users from serious real-world harms to public safety and democracy from misleading content and to safeguard the overall information ecosystem from threats resulting from the use of AI.

Providing users with increased transparency about the content they are encountering can support users' engagement with synthetic content. Ofcom should consider the role that labelling, displaying provenance and detection of manipulated content by platforms can have on the public's ability to make informed decisions regarding the content they view.

[12] Ofcom, 2024, Children and parents: media use and attitudes report 2024

Ofcom may also benefit from considering the potential of tools to detect AI-generated content reflecting them in its codes of practice and guidance. The efficacy of such tools should be kept under review, to ensure that their limitations are well understood by users. In conjunction with its wider research work in this space to understand the nature of these threats, Ofcom should also continue gathering evidence on how confident users are in identifying AI content and the extent to which they trust content generated by AI.

5. Technology and innovation

Technology is vital to protecting users online and for platforms fulfilling their duties under the Act. Innovation is also an important lever to support agile regulation and one tool among several that we must harness to ensure the continual strengthening of our online safety regime. Ofcom should ensure expectations on very low-risk services are proportionate, providing them with the freedom to innovate without imposing overly burdensome requirements or enforcement actions where there is little risk or evidence of harm. Ofcom should instead foster innovation and growth by focusing its regulatory efforts on high-risk services, whilst continuing to ensure that high-risk services are able to innovate in order to keep their users safe.

In addition to the innovation that Ofcom encourages within regulated companies, the UK safety tech sector has an important role to play by developing innovative solutions to support platforms, improve online safety outcomes and enable agile regulation. The sector has seen impressive growth since its inception and research from our Sectoral Analysis indicates that it remains on track to reach £1 billion in annual revenues by the mid-2020s, with a compound annual growth rate of circa 25% since a baseline was taken in 2019.

It is important that both in-house and third-party innovation continues at pace given the rate at which new threats are emerging and the importance of user safety. The government is committed to working with partners, including Ofcom, to achieve this, and the government's strategic priorities in relation to technology and innovation are set out below.

5.1 Encouraging innovation in safety technology to improve experience of all users online

The government and its partners have backed the development of innovative third-party solutions to online harms. This has included through challenge funds to protect children online and work to understand provision across the safety tech sector. We will continue to work with industry, regulators and international actors to support innovation through initiatives such as hackathons, innovation challenges and grant funding programmes. Platforms should also be encouraged to invest in innovation and do so in a way that is transparent so views on best practice are developed and shared across the sector.

The government will also support, alongside Ofcom, the development of the evidence-base of technology gaps and areas where innovation is necessary to meet our online safety aims. Alongside conducting new research and using horizon scanning functions, the government and Ofcom would benefit from mutually evaluating existing interventions. This includes developing a better understanding of the scale and impact of access to data on the development of online safety tools and possible solutions for addressing it. This should include monitoring the role that algorithms can play in supporting users who are predisposed to seeking out harmful content.

Furthermore, we would encourage Ofcom to build on its plans for its Online Safety Technology Lab to support innovation. We will continue to monitor trends within the safety tech ecosystem to ensure the conditions for innovation to take place remain.

5.2. Driving adoption of safety technologies by online services to improve experience and support compliance

It is not enough that new, innovative solutions to known problems exist - online service providers must also adopt and deploy these solutions to improve user safety.

Under the Act, Ofcom can recommend the adoption of technologies to services in its codes of practice and guidance to outline a clear path for industry to take to comply with the duties in the Act. The government will be a partner in helping Ofcom understand the effectiveness of different technologies and approaches and encourages Ofcom to be ambitious in its recommendations and ensure they maintain pace with technology as it develops.

We expect that this will not only raise the floor of what is expected from online services but will also raise the ceiling of what is possible by nurturing a culture of effective innovation in practice.

Service providers should also be able to have confidence that the tools they adopt will be resilient and not create friction that disproportionately impacts the user experience. To that end, we want to encourage a climate where interoperability is improved. This will require greater cooperation from online services, as well as domestic and international efforts. The government and Ofcom will need to be forward-leaning in positioning the UK as a leading contributor in these discussions and encourage discourse and collaboration domestically while actively participating in international fora, including the Global Online Safety Regulators Network and International Working Group on Age Verification.

5.3 Supporting the development of more effective age assurance technologies

Innovation is particularly important for age assurance technologies. While effective age assurance solutions exist, the government recognises the importance of continued innovation to maximise their effectiveness, as well as consistent standards for these technologies. This is so that age assurance solutions preserve users' privacy to a high standard, while ensuring the outcome of effective protection of all children online. This includes making sure that users of all backgrounds can access age-appropriate experiences online and have an accessible user experience.

We want to ensure that there is space in the regulatory landscape for the innovation of age assurance solutions. Through codes of practice and guidance, Ofcom is responsible for recommending age assurance technologies to regulated services to support compliance with their duties under the Act.

It is important that Ofcom's recommendations are kept up to date to ensure that they are reflective of new technological developments and capabilities. This includes working to support standards on age assurance technologies, including standards for accuracy. We will support Ofcom in continuing to develop its understanding of these technologies through sharing knowledge and growing the evidence-base. This way Ofcom can create a space for continued ambition in age assurance technologies and deliver age-appropriate online experiences for children.

E03303156

978-1-5286-5464-7