Witness Name: Dr Jon Higham
Exhibits: JH/01 – JH/28
Dated: 8 September 2025

THE SOUTHPORT INQUIRY

WITNESS STATEMENT OF DR JON HIGHAM

I, Dr Jon Higham will say as follows: -

INTRODUCTION

1. I am a director of policy development in Ofcom's Online Safety Group. I have been working on online safety regulation for 6 years, including 3 and a half years in my current role. I led our work to develop the first set of codes of practice and guidance setting out what online service providers should do to comply with their duties to protect people from illegal content under the Online Safety Act (OSA). Prior to that I played a significant role in our engagement with Government on the drafting of the OSA. Before joining the Online Safety Group I spent over 10 years working in a range of other parts of Ofcom.
2. This witness statement is made to assist the Southport Inquiry (the "Inquiry") with the matters set out in the Rule 9 Request dated 12 August 2025.

STRUCTURE OF THIS WITNESS STATEMENT

3. The remainder of this witness statement is in four sections, as follows:
    a) Section 1 – Role and Remit/ Responsibilities of Ofcom
    b) Section 2 – Online Harms and the Online Safety Act 2023
    c) Section 3 – Reflection on events
    d) Section 4 – Improvements and any further matters
    e) Section 5 – Disclosure: documents and communications
4. It has 1 Annex:
    a) Annex 1 - Index to the witness statement of Jon Higham

SECTION 1 – ROLE AND REMIT/ RESPONSIBILITIES OF OFCOM

About Ofcom

5. Ofcom is a statutory corporation established by the Office of Communications Act 2002.
6. Ofcom is the independent regulator for the UK communications industries, including post, telecommunications, network security, broadcasting, on-demand programme services, radio spectrum and online services.
7. Ofcom's principal duty, as set out in section 3 of the Communications Act 2003, is to further the interests of citizens in relation to communications matters; and to further the interests of consumers in relevant markets, where appropriate by promoting competition.

Ofcom's role as the online safety regulator

8. From 1 November 2020, Ofcom was the regulator of video-sharing platforms ('VSPs') in the UK under Part 4B of the Communications Act 2003, until 25 July 2025 when the VSP regime was repealed. From 26 October 2023, Ofcom has been the UK's online safety regulator under the OSA with a broader suite of powers and duties to regulate online services in the UK. Further detail about these regulatory frameworks and Ofcom's role are set out in Section 2 below.
9. The OSA requires online services that host user-generated content and search services to protect their users in the UK from illegal content, and in the case of children, from content that is harmful to them, such as violent content or content related to abuse and hate. The OSA places duties on providers of regulated online services to assess and manage safety risks arising from content and conduct on their sites and apps. It does not expect all harmful and illegal content to be eradicated online, but it does expect services to have suitable measures to protect adults and children in the UK, for example measures allowing for the swift take down of illegal content and the use of highly effective age assurance to prevent children from accessing content harmful to children. Ultimately the OSA seeks to drive services to prioritise safety in the design of their products and wider systems. As part of this, Ofcom is required to publish codes of practice and guidance to assist service providers in understanding their regulatory obligations and how they can comply, as well as enforcing against service providers where they fail to do so.
10. In contrast to our role as the broadcast content regulator, where we do consider

complaints about individual programmes, it is not Ofcom's role as the online safety regulator to adjudicate on complaints brought by individual users about particular pieces of content or services, nor to instruct regulated services to remove particular pieces of content. Ofcom's powers under the OSA do not enable us to do this. Securing outcomes which uphold the importance of freedom of expression and privacy is embedded within the OSA and within our implementation of the regime, which has ensured that our codes of practice and guidance have been rigorously assessed to ensure consistency with these rights.

11. Our role is to ensure that regulated online services improve the systems and processes they use to protect their users in the UK, and reduce the risks posed by online content that is illegal and harmful to children. Seeking systemic improvements will reduce risk and harm at scale, rather than focusing on individual instances. Organisationally, Ofcom's work on online safety is led out of Ofcom's Online Safety Group, with input from cross-functional teams such as Legal, Enforcement, Economics & Analytics, and Ofcom's strategy and research teams.

Ofcom's relationships and work with other bodies

12. Ofcom is independent from the Government and accountable to Parliament and through the Courts. To perform our role effectively we need to engage openly and constructively with the UK and devolved Governments. Ofcom's existing Framework Agreement [Exhibit JH/01 - **OFC000003** sets out the broad framework in which Ofcom operates in relation to carrying out its statutory functions, however it does not convey any legal powers or responsibilities. When we take decisions under the OSA, including in relation to the exercise of our enforcement functions, we do so independently.
13. The Secretary of State for Science, Innovation and Technology also has a number of statutory responsibilities under the OSA and we therefore collaborate in relation to the exercise of these functions in our work implementing the OSA, along with the Home Office. Ofcom, DSIT and the Home Office are members of the Joint Steering Group which has governance oversight for the implementation of the OSA. We meet with other departments such as the Ministry of Justice and the Department for Culture, Media and Sport on an ad-hoc basis to discuss mutual policy interests on online safety.
14. On 2 July 2025, the Government designated their Statement of Strategic Priorities ('SSP') for online safety under section 172 of the OSA. In accordance with our duties under section 92 of the OSA we must have regard to the SSP when carrying

out our online safety functions and we must explain in writing what we propose to do in consequence of the SSP. We published our explanation as to how we will have regard to the SSP on 25 July 2025, focusing in particular on the work we will carry out this year that is relevant to the priorities set out in the SSP [Exhibit JH/02 - **OFC000004**

15. Ofcom also has a good working relationship with a range of other online harms stakeholders across government, policing and civil society, is represented on key governance fora across the serious organised crime and terrorism portfolios and sits on several cross-government strategic groups on online harms issues. In particular, Ofcom's Online Safety Group manages relationships with Home Office harms policy units, the National Crime Agency, Counter Terrorism policing and NPCC leads. This includes working as part of a multi-agency task force to develop a strong intelligence picture of online harms, deliver a coordinated and effective response to online harm and share insights to support the operational delivery of the online safety regime. Ofcom is also working with the Violent Fixated Individuals ('VFIs') unit in the Home Office to understand the online pathways and enablers around VFIs. Through this, we are keen to understand the role played by in scope services in relation to a number of harm areas (including illegal content relating to hate speech, child sexual abuse and violence) and identify opportunities to drive down this harm through the online safety regime.
16. The Online Safety Group also manages partnerships with other regulators and key civil organisations operating in the online safety space to support and inform our broader policy development work. This includes being a member of the Digital Regulation Cooperation Forum, alongside the Information Commissioner's Office (ICO), Competition and Markets Authority and the Financial Conduct Authority. This forum aims to enhance regulatory coherence across its members remits, foster collaboration on shared challenges, and build collective expertise for effective regulation.
17. Our information sharing with public bodies is subject to the relevant statutory provisions which govern our handling of information, and is managed via a suite of memoranda of understanding, to enable secure and confidential information sharing between organisations for the purposes of facilitating the exercise of Ofcom's online safety functions. Such frameworks might cover any legal basis and restrictions for onward disclosure as well as working arrangements and agreed processes for data handling (see for example Ofcom's Memorandum of Understanding with the ICO [Exhibit JH/03 - **OFC000005**) The Government security classification system is applied to protect information appropriately and it is securely stored on Ofcom

systems.

SECTION 2 – ONLINE HARMS AND THE ONLINE SAFETY ACT 2023

The regulatory framework for online safety

18. Prior to 1 November 2020, there was no regulatory regime in the UK specifically for online safety. The general law applied, for example data protection and criminal laws.
19. Ofcom had (and continues to have) a duty under section 11 of the Communications Act 2003 to promote media literacy. It requires Ofcom to take such steps, and to enter into such arrangements, as appear to us calculated:
    a) to bring about, or to encourage others to bring about, a better public understanding of the nature and characteristics of material published by means of the electronic media;
    b) to bring about, or to encourage others to bring about, a better public awareness and understanding of the processes by which such material is selected, or made available, for publication by such means;
    c) to bring about, or to encourage others to bring about, the development of a better public awareness of the available systems by which access to material published by means of the electronic media is or can be regulated;
    d) to bring about, or to encourage others to bring about, the development of a better public awareness of the available systems by which persons to whom such material is made available may control what is received and of the uses to which such systems may be put; and
    e) to encourage the development and use of technologies and systems for regulating access to such material, and for facilitating control over what material is received, that are both effective and easy to use.
20. The EU's Audio-Visual Media Services Directive was amended from 18 December 2018 and implemented into domestic law on 1 November 2020 under Part 4B of the Communications Act 2003. This established a new regime for regulating VSPs.
21. The OSA received Royal Assent on 26 October 2023. Ofcom has been working to implement the regime, and our Illegal Harms and Protection of Children Codes of Practice and Guidance were published in December 2024 and April 2025 respectively, and are now in force. Further parts of the regime are in the process of being implemented. The timescales for the implementation of the OSA are explained in further detail at paragraphs 44-55 below. At the time of the Southport

attack in July 2024, the only online safety regulations in force were those relating specifically to VSPs which we discuss below.

Ofcom's work on VSP regulation

22. As explained above, from 1 November 2020 until 25 July 2025 there was a regulatory regime for VSPs which fell within the UK's jurisdiction. Broadly speaking, it is my understanding that such a provider fell to be regulated under this regime if it was established in the UK, or if a group undertaking of the provider was established in the UK and the provider did not fall to be regulated by an EEA state under the Audio-Visual Media Services Directive.
23. The types of service which may have met the definition of a VSP (see section 368S of the Communications Act 2003) would have included services which hosted videos as their main activity and allowed users to upload videos and engage with other users' content.
24. As at July 2024, I understand the list of notified VSPs was as set out in [Exhibit JH/04 **OFC000006** and included TikTok, Snapchat, OnlyFans and BitChute, among others. This means that some of the biggest and most well-known services were not within the UK's jurisdiction for the purposes of VSP regulation.
25. The regime covered two areas which I refer to together as 'harmful material'. Ofcom provided guidance [Exhibit JH/05 - **OFC000007** on these terms but in summary these were:
    a) Regulated VSPs had to protect all users from "relevant harmful material". This was video material likely to incite violence or hatred against protected groups, and content which would be considered a criminal offence under laws relating to terrorism; child sexual abuse material; and racism and xenophobia.
    b) Regulated VSPs had to protect under-18s from "restricted material". This was video material containing R18 or unclassified material, and other material that might impair their physical, mental, or moral development.
26. Schedule 15A of the Communications Act 2003 listed measures that, pursuant to section 368Z1 of that Act, VSP providers were required to take, if appropriate, to fulfil their duties to protect users from harmful material. They included:
    a) Having, and effectively implementing, terms and conditions for harmful material;
    b) Having, and effectively implementing, flagging, reporting or rating mechanisms;
    c) Applying appropriate access control measures to protect under 18s, such as age assurance and/or parental control measures;
    d) Establishing easy-to-use complaints processes; and

e) Providing media literacy tools and information.

27. Section 368Z1(4) set out that a measure was appropriate for a certain provider if it was practicable and proportionate for that provider to implement it, considering factors including the size and nature of its platform; the type of material on the platform and the harm it might cause. Whilst providers were required to ensure that 'restricted material' was subject to the strictest measures (e.g. age verification), this duty was subject to the caveat that providers were not under any general duty proactively to look for illegal or harmful content or activity on their platform, for example by using forms of proactive technology to do this (see section 368Z1 of the Communications Act 2003 and Article 15(1) of Directive 2000/31/EC).

28. We published guidance to help providers understand the complex scope and jurisdictional criteria of the legislation [Exhibit JH/06 - **OFC000008**], and issued publications to provide clarity on what the new framework would mean for providers in scope – such as the 'quick guide' to the new regulations [Exhibit JH/07 - **OFC000009**].

29. Under the VSP legislation, Ofcom also published reports about the measures taken by platforms for the purposes of protecting users from videos containing harmful material. During this time, relevant VSPs took measures such as limiting the amount of content that could be viewed by users without an account, asking users to self-declare age when registering for an account, presenting users with terms and conditions upon registration prohibiting certain material, and categorising content based on suitability for those aged under or over eighteen [Exhibit JH/08 - **OFC000010**].

30. We understand that prior to the attack on 29 July 2024, AR accessed content which included terrorist material and depictions of violence. I do not know whether or not this material was accessed on a regulated VSP, nor have I seen copies of the material myself. I can however explain what the expectations would have been had it been in scope of VSP regulation. Based on the description of the material provided by the Inquiry it is plausible that some of the content would have amounted to "restricted material" and/or "relevant harmful material". As outlined above, assuming such material had been made available on a regulated VSP, the precise expectations on the service in question would have depended on what measures would have been appropriate, which would itself depend on a number of factors, including the size and nature of the platform. In general terms, Ofcom would have expected appropriate measures to have been in place by providers of regulated VSPs to limit children's access to video material including terrorist material and detailed portrayals of violence – but this does not mean that such

material would never have been accessible to children at all. As noted above at paragraph 26, VSP legislation allowed providers to implement measures, such as establishing mechanisms for flagging and reporting and having systems for obtaining assurance as to the age of potential viewer. However, it may not have been appropriate under VSP legislation for all providers of regulated VSPs to have these measures in place. Additionally, where a provider did determine that a particular measure would have been appropriate, the duty to take appropriate measures did not extend to an obligation on platforms to pro-actively monitor for harmful material.

The Online Safety Act 2023 - overview

31. The OSA gave new powers to Ofcom to regulate companies that provide three categories of internet service (known as 'regulated services'):
    a) user-to-user services- these are services on which users can upload or share content (user-generated content) with other users of the service – for example, social media services, video-sharing services, messaging services and online forums, online marketplaces, gaming services, dating services, among others;
    b) search services – these services include search engines which enable users to search more than one website or database, and
    c) online services on which the provider of the service publishes or displays pornographic content[1].
32. Unlike the VSP regime, the OSA regulates services that are provided outside the UK as well as those provided inside the UK, so long as the service has 'links with the UK' (sections 4 and 204). 'Links with the UK' means where a service has a significant number of UK users, for which the UK is a target market, or (for user-to-user and search services) which is capable of being used in the UK by individuals and presents a material risk of significant harm to individuals in the UK.
33. The general purpose of the OSA is set out in section 1: making the use of regulated internet services safer for individuals in the United Kingdom. The duties imposed on providers by the OSA seek to secure (among other things) that regulated services are safe by design and designed and operated in such a way that a higher standard of protection is provided for children than for adults, users' rights to freedom of

[1] These services are subject to separate duties to user-to-user and search services, set out in sections 79 to 81 in Part 5 of the OSA. In essence, providers of these services must use highly effective age assurance to ensure children cannot normally access pornographic content.

expression and privacy are protected, and transparency and accountability are provided in relation to those services.

34. The range of harms which the OSA covers is broad. The OSA defines well over 100 offences as 'priority offences'. Broadly speaking these priority offences can be divided into offences related to the following areas: terrorism, child sexual exploitation and abuse, threats, abuse, hate and harassment, suicide, drugs and psychoactive substances, firearms and other weapons, illegal immigration, human trafficking, adult sexual exploitation, extreme pornography, intimate image abuse, proceeds of crime, fraud and financial services offences, foreign interference and animal welfare. Other criminal offences could give rise to "non-priority" offences, including an offence relating to improper use of a public electronic communications network which can cover online content depicting the torture of humans and/or animals. As set out below, the duties on providers to protect users are greater for priority offences than for non-priority offences.

35. In addition to the illegal content types referred to above, the OSA designates a number of types of lawful content as harmful to children. For the purposes of the protection of children duties, there are three types of content deemed to be "content harmful to children". "Primary priority content" is defined in section 61 of the OSA and relates to pornography, suicide, self-injury, and eating disorder or behaviours associated with an eating disorder. "Priority content" is defined in section 62 of the OSA and relates to abuse and hate, bullying, violence, harmful substances and dangerous stunts and challenges. Other content harmful to children is known as "non-designated content harmful to children". This is content which presents a material risk of significant harm to an appreciable number of children in the UK (section 60(2)(c)). As explained below, the safety duties in relation to primary priority content are more onerous than those for other types of content harmful to children.

36. The OSA imposes a range of duties on regulated service providers. For the purposes of this written statement, the key ones for the Inquiry to be aware of are:

    a) Duties for both user-to-user and search services to assess the risk of illegal content occurring by means of the service (sections 9 and 26 of the OSA);

    b) Duties for both user-to-user and search services to put in place proportionate systems and processes to reduce the risk of individuals encountering types of illegal content defined in the Act as priority illegal content and to effectively mitigate and manage the risks identified in the illegal harms risk assessment (section 10(2) and 27(2) of the OSA);

    c) A duty for user-to-user services to take down any illegal content down swiftly when the service provider becomes aware of it (section 10(3)(b) of the OSA);

d) A duty for all regulated services to assess whether children are likely to access the service (section 36 of the OSA);
e) Duties for providers of all regulated services likely to be accessed by children, to assess the risk of children encountering harmful content by means of the service (section 11 and 28 of the OSA);
f) Duties for user-to-user services likely to be accessed by children to:
    - put in place proportionate systems and processes designed to prevent children of any age from encountering certain types of content which the OSA has defined as primary priority content (section 12(2)(a) of the OSA);
    - put in place proportionate systems and processes to protect children in age groups judged to be at risk of harm from other content that is harmful to children from encountering it by means of the service (section 12(2)(b) of the OSA); and
    - have systems and processes that allow users to report and make complaints about content harmful to children being present on a service (section 20(1) and (5) and section 21(2) and (5) of the OSA).

37. Providers are also subject to additional duties relating to freedom of expression and privacy. In summary, when deciding on, and implementing safety measures and policies, they must have particular regard to the importance of protecting users' right to freedom of expression and protecting users from a breach of any statutory provision or rule of law concerning privacy that is relevant to the use of a service (see section 22 and section 33 of the OSA).

38. We have published a number of pieces of guidance setting out how service providers should comply with these duties. These include:
a) Illegal Content Judgements Guidance and Guidance on content harmful to children. These pieces of guidance are designed to assist providers in making judgements about whether pieces of content are illegal or constitute content harmful to children. The illegal content judgements guidance explains that content should be considered as 'illegal content' where there are reasonable grounds to infer that a) the conduct element of a relevant offence is present or satisfied; b) the state of mind element of that same offence is present or satisfied; and there are no reasonable grounds to infer that a relevant defence is present or satisfied (see section 192 of the OSA). These pieces of guidance make clear that context is key when making content judgements and providers should consider rights to freedom of expression. Given this, these guidance documents also highlight that some forms of content are unlikely to amount to

illegal content or content harmful to children, such as journalistic or academic content[2].

b) Guidance on how service providers should do their risk assessments. This sets out that service providers should identify the risks of illegal content and content harmful to children that could occur on their services; assess the probability and impact of these risks occurring; identify the steps they are going to take to manage the risks; and record and regularly review their risk assessment;

c) Illegal Harms codes of practice and Protection of Children codes of practice. These codes of practice respectively set out what steps we consider service providers should take to fulfil their duties to mitigate risks relating to illegal content and to protect children from content which is harmful to them. The codes are a safe harbour. That is to say, if service providers follow the steps set out in our codes, they are deemed to be compliant with their safety duties under the OSA. However, it is open to service providers to deviate from the codes and take alternative measures to comply with their duties under the OSA, provided that these alternative measures are sufficiently rigorous to meet the terms of the OSA.

39. The OSA requires Ofcom to ensure that measures we recommend are designed to account for the importance of rights to freedom of expression and privacy and are proportionate. Our approach to the codes of practice recognises that the size, capacity and risks of services differ widely. The measures we recommend in codes therefore vary depending on the risks the service poses, with the most extensive expectations on the riskiest services (please see Ofcom's 'Approach to developing codes measures' for Illegal Harms [Exhibit JH/09 - **OFC000011** and our 'Codes at a glance' document for Protection of Children [Exhibit JH/10 - **OFC000012**.

40. The Illegal Harms codes of practice include a number of recommendations as to what service providers should do to meet their duties in relation to illegal harms. For example:

(a) Service providers should have easy to use reporting and complaints functions, so their users can more easily report content which could be illegal or harmful to children.

(b) For user-to-user services, providers should, as part of having a content moderation function, have systems and processes designed to review and assess content the provider has reason to suspect may be illegal content.

[2] News publisher content is excluded from the definition of regulated user-generated content and search content in the Act and therefore not subject to the safety duties about protecting children and illegal content (sections 55-56 and 57(2)(b) and (c) of the OSA)

Related to this, larger and riskier service providers should resource and train their content moderation teams appropriately.

(c) For user-to-user services, providers should as part of their content moderation, have systems and processes designed to swiftly take down illegal content, unless it is currently not technically feasible to achieve this outcome.

(d) User-to-user services should use a technology called hash matching to detect child sexual abuse material ('CSAM'), so it can be removed.

(e) For search services, providers should, as part of a search moderation function, have systems and processes designed to review, assess and where relevant take appropriate moderation action in relation to search content which the provider has reason to suspect may be illegal content.

(f) For large general search services, providers should have a function that allows UK users a means to easily report predictive search suggestions which they consider direct users towards priority illegal content.

41. Ofcom's Protection of Children codes of practice recommend a number of measures for both user-to-user and search services that are likely to be accessed by children. These include but are not limited to:

(a) For all services, providers should have content moderation processes in place to review, assess and take swift and appropriate action on content identified as content harmful to children.

(b) The use of highly effective age assurance for services where the principal purpose is the hosting or dissemination of primary priority or priority content or where the service does not prohibit primary priority or priority content.

(c) Providers of user-to-user services that operate recommender systems and are medium or high risk for content harmful to children should exclude in children's recommender feeds primary priority content and exclude or give a low degree of prominence to other content that is harmful to children.

(d) Providers of large general search services with a predictive search functionality should enable users to report predictive search suggestions relating to content harmful to children. If the provider identifies a clear and material risk from the predictive search suggestion, they should take appropriate steps to ensure it is not recommended to any users.

42. We are currently consulting on making some targeted additions to our Illegal Harms and Protection of Children codes of practice. These proposed additions include adding a recommendation that: (i) service providers should assess whether accurate and effective automated tools, including Artificial Intelligence, to proactively detect certain types of illegal content and content harmful to children are

available; and (ii) where such tools are available they should use them. This measure includes CSAM content, suicide and self-harm content and fraudulent content.

43. We have also consulted on draft guidance setting out how providers can take action against harmful content and activity that disproportionately affects women and girls. This draft guidance brings together relevant measures and guidance across Illegal Harms and Protection of Children and includes additional examples of good practice for providers. Taking a safety-by-design approach we are seeking to demonstrate how providers can embed the concerns of women and girls throughout the operation and design of their services, features and functionalities.

Implementation of the Online Safety Act – overview

44. 26 October 2023 marked the commencement of some, but not all of Ofcom's powers and functions under the OSA. In particular, Ofcom could not, at this time, take enforcement action in relation to the Illegal Harms and Protection of Children duties. We have moved quickly to implement the new rules, which are being rolled out in three phases, with the timing driven by the requirements of the OSA and relevant secondary legislation. The first phase of implementation related to illegal harms. The second phase related to protection of children. The third phase relates to a set of additional duties the OSA imposes on what it terms categorised services. In line with the statutory deadlines imposed by Parliament under the OSA, we prioritised the completion of codes and guidance to tackle illegal harms and create a safer life online for children.

45. The implementation of each phase of the new rules required thorough consultation (which we could not formally launch until after the Act came into force), drafting and finalisation of the codes, and parliamentary approval prior to the codes coming into force. As we explain in more detail below some elements of our work are dependent on secondary legislation which was only recently passed. Moreover, some elements of our work have been delayed by legal proceedings. For these reasons, the process of implementing the regulations takes a number of years. However, we have sought to progress every stage of implementation as quickly as practicably possible – for example, we published our first consultation just weeks after the OSA came into force.

46. As set out in further detail below, we have completed the first two phases of implementation of the new rules, relating to Illegal Harms and Protection of Children. The codes of practice for both of these elements of the regime are now in

force and we are working to ensure service providers are complying with them. Implementation of phase 3 of the new rules will introduce additional duties for 'categorised services' which we explain in further detail below.

47. Below we set out our written chronology of our implementation of the OSA. A visual aid detailing Ofcom's timeline for implementation for the first two phases is included as [Exhibit JH/11 **OFC000013**].

Detailed chronology – implementation of illegal harms rules

48. On 9 November 2023, Ofcom consulted on our first suite of regulatory products required to bring the new regime into effect, focusing on illegal harms:
    - Illegal harms Register of Risks,
    - Illegal harms Risk Assessment Guidance including Risk Profiles,
    - Illegal content Codes of Practice for user-to-user and search services,
    - Record keeping and review guidance,
    - Enforcement Guidance,
    - Illegal content judgments guidance, and
    - Guidance on content communicated 'publicly' and 'privately' under the OSA.
49. On 16 December 2024, having considered consultation responses, Ofcom published our final decisions and regulatory products in relation to Illegal harms. This included our final Illegal Content Judgements Guidance[3], Register of Risks, and Illegal harms Risk Assessment Guidance [Exhibits JH12-JH/15 - **OFC000014-17**] The publication of our Illegal Harms Risk Assessment Guidance triggered the beginning of a three-month period for regulated service providers to carry out their first illegal content risk assessment, i.e. by 16 March 2025. On 16 December 2024, the Secretary of State laid the codes for illegal content duties before Parliament for a period of 40 days. Following approval by Parliament, the codes then came into force on 17 March 2025, and the illegal content safety duties also came into effect from this point.
50. As detailed at paragraph 42, on 30 June 2025, Ofcom published a consultation on a package of additional proposals for recommendations of measures to keep users safe online from illegal content and content that is harmful to children. I have exhibited the main consultation document [Exhibit JH/16 - **OFC000018**] and our

[3] The Illegal Content Judgements Guidance published on 16 December 2024 has since been superseded on 30 July 2025, in order to correct a minor technical inaccuracy in the initial publication

proposed additional Codes for user-to-user services for illegal harms [Exhibit JH/17 - **OFC000019** and protection of children [Exhibit JH/18 - **OFC000020**. The consultation will close on 20 October 2025.

Detailed chronology – implementation of protection of children rules

51. The second phase of work related to protecting children against harmful content.
52. On 5 December 2023 we published our draft guidance for online pornography services on their new duties to use age assurance to prevent children from accessing pornographic content.
53. Our main consultation on the protection of children codes and guidance was published on 8 May 2024 and covered:
    a) Children's Register of Risks,
    b) Children's Risk Assessment Guidance including Risk Profiles,
    c) Protection of children Codes of Practice for user-to-user and search services,
    d) Guidance on content harmful to children,
    e) Children's access assessments guidance, and
    f) Guidance on highly effective age assurance for Part 3 services.
54. On 16 January 2025, we published our final guidance on highly effective age assurance for online pornography services [Exhibit JH/19 - **OFC000021** The duties on these services came into effect on 17 January 2025. Having considered responses to the consultation, we also published our final decision on the children's access assessment guidance on 16 January 2025 [Exhibit JH/20 - **OFC000022** This triggered a three-month period for providers to carry out their children's access assessments, which were to be completed by 16 April 2025.
55. On 24 April 2025, again having considered responses to the consultation in relation to protection of children duties, Ofcom published our final decisions. This included our final children's Risk Assessment Guidance [Exhibit JH/21 - **OFC000023** the publication of which triggered the beginning of a three-month period for regulated service providers to carry out their first children's risk assessment (i.e. by 24 July 2025). On 24 April 2025, the Secretary of State laid the codes for the protection of children before Parliament for scrutiny for a period of 40 days. Following Parliamentary approval, the protection of children Codes of Practice came into force on 25 July 2025 [Exhibit JH/22 - **OFC000024** and [Exhibit JH/23 - **OFC000025** and the duties on services likely to be accessed by children came into effect on the same date.

Duties for 'categorised' providers

56. There are additional duties for providers of certain kinds of regulated user-to-user and search services, known as "categorised services", which meet certain thresholds set out in secondary legislation, namely the Online Safety Act 2023 (Category 1, Category 2A and Category 2B Threshold Conditions) Regulations 2025 (SI 2025/226) ('the Regulations')[4]. The additional duties for Category 1 services relate to the inclusion of the findings of risk assessments in terms of service (sections 10(9) and 12(14)), user empowerment (section 15), content of democratic importance, news publisher content, journalistic content (sections 17 to 19), complaints procedures (section 21(6)), carrying out impact assessments relating to freedom of expression and privacy (section 22(4)-(7)), fraudulent advertising (sections 38 to 40), user identity verification (section 64), a duty not to take certain actions except in accordance with terms of service (sections 71 and 72), disclosure of information about use of a service by deceased child users (section 75) and transparency reporting (section 77). The duties about summarising findings of risk assessments (section 27(9) and 29(9)) and fraudulent advertising duties (section 39) also apply to 'Category 2A services' and the duties relating to transparency, and deceased child users also apply to Category 2A services[5] and 'Category 2B services'. These duties are not currently in effect, pending further steps to be taken to implement the regime, as explained as follows.

57. On 25 March 2024, as required by Schedule 11 to the Act, Ofcom published research and advice to the then Secretary of State on the thresholds for providers to be 'categorised' under the OSA, for the Secretary of State to consider before deciding on the conditions to set out in secondary legislation on the applicable thresholds. Following the General Election, the draft statutory instrument containing the proposed regulations were laid before Parliament by the new Secretary of State on 16 December 2024. The Regulations came into force on 27 February 2025.

58. Ofcom is required to publish and maintain a register of services categorised as Category 1, Category 2A and 2B on the basis of the thresholds set out in secondary legislation. Ofcom is also required to publish a list of emerging Category 1 services. Ofcom is also required to publish codes of practice and guidance for Category 1, 2A and 2B services relating to the additional duties on categorised services. Ofcom has

[4] Category 1 and 2B means regulated user-to-user services which meet the Category 1 or 2B threshold conditions in relation to the user-to-user part of the service, as applicable.
[5] Category 2A means a regulated search of combined services which meets the Category 2A threshold conditions in relation to the search engine of the service.

been progressing our work on the register and consultation on the codes of practice and guidance relating to the additional duties on categorised services as quickly as possible. We had originally hoped to publish the register in summer 2025 with a view to publishing the consultation on the codes of practice and guidance in Q1 2026 and to finalising the codes of practice and guidance in 2027 [Exhibit JH/24 - **OFC000026**]. However, the Wikimedia Foundation, which is the provider of the Wikipedia service, brought a judicial review challenge against the Regulations, which has led to some delays to the timetable. This challenge was dismissed on 11 August 2025. Ofcom is still in the process of considering the implications of the judgment on Ofcom's work and what this means for the overall timetable. I would be happy to provide a further update on this to the Inquiry if helpful when possible. I would note, however, that we have in the meantime published our final transparency reporting guidance on 21 July 2025 [Exhibit JH/25 - **OFC000027**].

Ofcom engagement with regulated services and approach to compliance

59. Ofcom's powers to intervene in relation to online safety extend only to the functions and powers accorded to us under the OSA and Communications Act 2003. As set out above Ofcom's Codes for Illegal Harms and Protection of Children have been implemented as quickly as possible, in order that we could begin to drive improvement by service providers, including by exercising Ofcom's compliance monitoring and enforcement powers. We set out below the various work that is currently underway.
60. We have been engaging with providers for a significant period of time, prior to Royal Assent of the OSA and throughout implementation. The central objective of this engagement has been to understand, assess and improve the technical safety mitigations these services have put in place to protect UK users from illegal online content, and to protect children from being exposed to content which is harmful to them. Ofcom has adopted a 'supervisory approach' with services to secure greater understanding of those services and their measures and to seek to secure improvements to improve online safety for users. Supervision is an approach used in some regulated sectors to oversee how an organisation complies with a set of rules or legislation. In line with the wider approach to delivering online safety, supervision focuses on the effectiveness of services' systems and processes in protecting their users, not on individual pieces of content.
61. This engagement has focused on a range of priority areas, which are often tailored to the circumstances and applicable risks for each service. However, this would

usually include illegal content, and risks to children. For example, Ofcom's work relating to 'small but risky' services requires a bespoke approach for which we have a dedicated supervision taskforce to target services that present a high risk of harm. This is intended to focus on high priority areas including terror and hate offences.

62. Since the OSA came into force at the beginning of this year, we have been clear in setting out our priority areas for compliance and the improvements we expect to see from industry. Ofcom's key areas of focus have included assessing providers of adult services' compliance with implementing highly effective age assurance, implementation of measures in respect of CSAM and assessment of whether providers are complying with their illegal content risk assessment duties under the OSA. We have used a combination of informal supervisory engagement and formal enforcement action to drive changes in these areas. As part of this work, we have opened a number of specific enforcement investigations against providers. For example, Ofcom's enforcement programme to monitor services compliance with their illegal content risk assessment and record keeping duties has resulted in an investigation in relation to Kick Online Entertainment S.A, in respect of the service Motherless. In June 2025 investigations were also opened under the CSAM enforcement programme into 7 providers for failure to adequately respond to a statutory request, failure to complete and keep a record of the illegal content risk assessment and implement measures recommended in the codes of practice or appropriate alternative measures. In July 2025, Ofcom opened investigations into five providers of adult services (8579 LLC, AVS Group Ltd, Kick Online Entertainment S.A,Trendio Ltd and Duplanto Ltd) for failure to comply with their duties under section 12 of the OSA to prevent children from encountering pornographic content through the use of highly effective age assurance. Ofcom have also opened investigations into Itai Tech Ltd and First Time Videos LLC for failure to comply with their duties under section 81 of the OSA to protect children from encountering pornographic content through the use of highly effective age assurance. Ofcom's approach to enforcement under the OSA is set out within our Online Safety Enforcement Guidance [Exhibit JH/26 - **OFC000028**].

63. The OSA is designed to make the use of certain internet services safer for people in the UK. The illegal content and children's safety duties under the OSA only apply to the design, operation and use of regulated services in the UK or as they affect UK users of these services (sections 8(3) and 25(1)). The measures in our codes of practice also only apply to the design and operation of services in the UK or as they affect UK users (Schedule 11, paragraph 11). This means that providers of

regulated services are not obliged to extend their safety measures to users based outside the UK.

64. Some service providers are approaching compliance with their duties under the OSA by 'geo-targeting' some, or all, of their safety measures at the UK only. Other services have chosen to entirely 'geo-block' the UK, effectively seeking to make their service unavailable to UK users; this is their choice. Geo-targeting and geo-blocking are typically achieved by applying the relevant measures or access restrictions only to users of the service with a UK-based IP address. We discuss the circumvention of geo-blocking further at paragraphs 72-74.

Illegal Harms and Protection of Children – Applicability

65. I understand that prior to the attack on 29 July 2024, AR accessed content which included terrorist material and depictions of violence. As noted above, the applicable duties under the OSA were not in force at this point in time. I also am not aware of precisely which services the content AR accessed was present on and have not seen this content myself. This being the case, it is difficult for me to give a view as to what the impact of regulation under the OSA would have been, had it been in force at the relevant time. I have therefore outlined how I would expect OSA regulation to apply in general in relation to this sort of content.

66. Without having seen the content, I cannot say for certain whether it would have fallen within scope of the OSA. However, based on the description of the material provided by the Inquiry it is plausible that some of the content may now fall within the scope of the OSA and would therefore be subject to the duties concerning illegal content and content harmful to children as set out above. The application of the duties in the OSA should materially reduce the probability of people encountering in scope content. However, they will not entirely eliminate the presence of such content online.

67. The extent to which content of the type AR viewed would be within scope of the OSA is necessarily dependant on a number of factors which I discuss below.

68. The first consideration is whether a service is regulated and if so to what extent they are subject to the duties under the OSA. See paragraphs 31-37 above which explains the types of services in scope of the OSA and the duties that apply to them. As explained above, the types of services in scope of the OSA include user-to-user services such as social media platforms like Facebook, Instagram and X, as well as video sharing platforms like YouTube. They also include search services like Google and Bing. However, where providers of online services publish their own

content on their service (or this is published on their behalf, for example for the purposes of their business), this is not generally in scope of the OSA.[6]

69. The second consideration is whether the content in question is regulated and if it falls under the definitions of illegal content or content that is harmful to children. If it does, then it will be subject to the relevant duties and should be covered by the steps that providers are taking to comply with these duties. See paragraphs 34-35 above which explain the type of content which is subject to regulation under the OSA and which are not.

70. As explained at paragraph 34, content is illegal content where this amounts to a relevant offence. Relevant offences comprise priority offences and other non-priority offences which I discuss at paragraph 34 of this statement. This would include offences related to terrorism and abuse and hate, as well as improper use of an electronic communications network, which can cover content depicting human torture and animal cruelty. For the purposes of the protection of children duties, some violent content including depictions of violence, or content showing hateful or abusive language may amount to priority content that is harmful to children under the OSA, as explained at paragraph 35 above. Violent content, as this relates to a person, is specifically defined as content which depicts real or realistic serious violence against a person and/or depicts the real or realistic serious injury of a person in graphic detail. This could include videos or images of stabbings, beheadings, torture and dead bodies. Content which is abusive or incites hatred is defined as being targeted specifically at specific characteristics, including race and religion. We would expect provides to consult Ofcom's Illegal Content Judgements Guidance and Ofcom's Guidance on content harmful to children, which I discuss at paragraph 38 of this statement, to assist as necessary in order to make content judgements.

71. As explained above, providers would need to take certain steps to comply with the duties under the OSA in respect of illegal content or content that is harmful to children. As noted above at paragraph 38 providers should determine which measures are appropriate for their service based on the findings of their risk assessment. Ofcom's codes of practice set out measures recommended for different types of service provider, including measures relating to content moderation (including taking down illegal content once they become aware of it),

[6] The exception is where the content published or displayed in the service by or on behalf of the service provider is pornographic – in which case the duties set out in Part 5 of the OSA apply – namely using highly effective age assurance to ensure that children are not normally able to access that content.

how they configure their recommender systems and use of age assurance to target safety protections at child users, all of which are intended to help keep users in the UK safer from illegal content and content that is harmful to them, including terrorism, violent content and types of hate speech. As discussed at paragraph 38, whilst these measures are recommended in Ofcom's codes, it is open to providers to employ alternative measures in order to secure compliance with the relevant duties.

Circumvention

72. Technologies are available, including VPNs, which can effectively 'mask' the IP address of the user of an internet service from the service provider. They can also be used so as to appear to the service provider to be based in a country other than the UK. These technologies are legal to use in the UK and are not regulated by Ofcom under the OSA. They may be used for a range of purposes including secure browsing on public networks and privacy protection. Based on our current evidence, 25% of UK internet users aged 16+ have used a VPN. However, the practical effect of using these technologies can be that people in the UK may still be able to access internet services despite service-level geo-blocks aimed at UK IP-addresses. It may also mean that they do not benefit from safety measures targeted at UK IP-addresses.
73. We expect service providers to refrain from hosting, sharing or permitting content that directs or encourages the use of a VPN or similar circumvention techniques (please see our guidance documents on highly effective age assurance, issued to Part 3 and Part 5 services [Exhibit JH/19 - **OFC000021**] and [Exhibit JH/27 - **OFC000029**]).
74. While VPN usage may allow determined and technically literate users to circumvent safety measures to find and access harmful content, we believe the OSA will still provide protections for the large majority of users, who do not routinely use VPNs in this way. We are aware that users do unfortunately encounter harmful content where they are not seeking it out, however the implementation of the required measures under the OSA will materially reduce the likelihood of this happening.

SECTION 3 – REFLECTION ON EVENTS

75. As noted above, the OSA regime was not in force in July 2024. While the VSP regime was in force, it was much more limited in scope than the OSA. This being

the case, I do not consider that there was any action that Ofcom failed to take or could have done differently in respect of the events of July 2024.

76. It is, however, important to reflect on the extent to which the actions we are taking under the OSA will reduce the probability of similar tragedies occurring in future.

77. For the reasons set out above, including the points I have made about circumvention, the OSA is not a panacea. It will not eliminate all risks relating to harmful content online. Indeed, its focus is to ensure that service providers are taking proportionate steps to manage risk rather than to completely eliminate risk.

78. Nonetheless, I am confident that by making service providers assess and take appropriate measures to mitigate risk the OSA will bring about material improvements to online safety. For example, many large services including Reddit, Discord and X committed to age-gating content prior to the deadline of 25 July 2025, and have since deployed highly effective age assurance measures on their sites.

79. It is not possible to say with certainty whether, had the OSA been in force, AR would have encountered the content that he did. What I can say with confidence is that, if the new regulations work as they should, the probability of any given individual encountering illegal content or any given child encountering content harmful to children will be materially lower than it would otherwise have been.

80. Finally, I think it is important to highlight that the OSA forms part of a broader ecosystem both within the UK and globally. Within the UK context, addressing safety risks and the drivers of extremism requires a 'whole of society' response. While Ofcom is and will continue to exercise its powers to ensure platforms identify and address the risks of harm from online content and conduct, as set out at paragraphs 12-17, Ofcom will continue to engage with Government and other stakeholders (including other public bodies and civil society) with the common goal of working together to secure a safer life online for users in the UK.

81. Beyond the UK, the services we regulate are available and used globally and the harms we seek to address are similar across the world. We have also been working with our regulatory counterparts in other jurisdictions, including Europe, the United States, and Australia, to gather and share evidence, experience and expertise, and to collaborate and coordinate our work where relevant.

SECTION 4 – IMPROVEMENTS AND ANY FURTHER MATTERS

82. Decisions on any future changes to legislation will be a matter for Government and Parliament, rather than for Ofcom.

83. It is premature to say whether the codes of practice and guidance we have published to date, or our strategy for driving compliance with the rules, could be improved. These are complex issues, involving highly dynamic technologies and user behaviours and engaging a number of human rights considerations that are sometimes in tension with each other. Our regulation is still at an early stage, and we therefore fully expect to iterate and improve regulation over time, within the existing legal framework. Indeed, we are already consulting on targeted additions to our Illegal Harms and Protection of Children codes of practice as explained at paragraph 42. To help us with this we have extensive research and monitoring and evaluation programmes. Through our approach to supervision, we will develop a more detailed understanding of the services Ofcom regulates in order to inform the development of our regulation in future. Where these highlight areas for improvement, we will not hesitate to adapt our approach.

84. Irrespective of the success of our initial interventions, we expect to have to update our codes and guidance over time to keep up with technological change and changes in the nature of the harms people are experiencing. To identify areas where we may need to make changes, we do an extensive amount of research and analysis to monitor technical developments and developments in the harms people are experiencing.

SECTION 5 – DISCLOSURE: DOCUMENTS AND COMMUNICATIONS

85. Ofcom has a power under section 100 of the OSA to require specified persons, including providers of regulated services, to provide us with information that we require for the purpose of exercising, or deciding whether to exercise, any of our online safety functions. Ofcom's 'online safety functions' are defined in section 235 of the OSA as comprising our functions under the OSA and functions that we have under specified provisions of the Communications Act 2003. Ofcom's online safety functions do not extend to obtaining information for the purposes of providing this to a public inquiry.

86. Ofcom also has a separate power under section 101 of the OSA to require specified persons, including providers of regulated services, to provide us with information for the purpose of:

    a) responding to a notice given by a senior coroner under paragraph 1(2) of Schedule 5 to the Coroners and Justice Act 2009 in connection with an investigation into the death of a child, or preparing a report under section 163 in connection with such an investigation;

b) responding to a request for information in connection with the investigation of a procurator fiscal into, or an inquiry held or to be held in relation to, the death of a child, or preparing a report under section 163 in connection with such an inquiry;

c) responding to a notice given by a coroner under section 17A(2) of the Coroners Act (Northern Ireland) 1959 (c. 15 (N.I.)) in connection with—

   i. an investigation to determine whether an inquest into the death of a child is necessary, or

   ii. an inquest in relation to the death of a child, or preparing a report under section 163 in connection with such an investigation or inquest.

87. Under section 101, the information we may require includes information about the use of a regulated service by the child whose death is under investigation, including:

   a) content encountered by the child by means of the service,

   b) how the content came to be encountered by the child (including the role of algorithms or particular functionalities),

   c) how the child interacted with the content (for example, by viewing, sharing or storing it or enlarging or pausing on it), and

   d) content generated, uploaded or shared by the child.

88. The exercise of the section 101 power is contingent on Ofcom being requested to provide information by a coroner or procurator fiscal (as relevant) in connection with an investigation into the death of a child under the powers outlined above.

89. We consider that the question of whether the powers under section 101 of the OSA are sufficiently broad is a matter for Government and Parliament.

90. Further information about Ofcom's information gathering powers relating to online safety, and how we expect to use them, is set out in Ofcom's Online Safety Information Guidance [Exhibit JH/28 - **OFC000030**].

Statement of Truth

I believe that the facts stated in this witness statement are true. I understand that proceedings may be brought against anyone who makes, or causes to be made, a false statement in a document verified by a statement of truth without an honest belief in its truth.

Signed:

Signature

Dated: __08/09/25____

Annex 1 – Index to the witness statement of Jon Higham

Exhibit No.	Inquiry reference No.	Document description
1.	OFC000003	Ofcom Framework Document, June 2016
2.	OFC000004	Letter to Government on the Statement of Strategic Priorities for Online Safety, 25 July 2025
3.	OFC000005	Memorandum of Understanding between the Information Commissioner and Ofcom, signed July 2019
4.	OFC000006	List of notified VSPs, July 2024
5.	OFC000007	Video-sharing platform guidance, 6 October 2021
6.	OFC000008	Statement: Video-sharing platforms – who needs to notify Ofcom, 10 March 2021
7.	OFC000009	Ofcom's video-sharing platform framework: a guide for industry, 6 October 2021
8.	OFC000010	Report: How video-sharing platforms (VSPs) protect children from encountering harmful videos, 14 December 2023
9.	OFC000011	Illegal Harms Statement – Our Approach to developing Codes measures, 16 December 2024
10.	OFC000012	Protecting children from harms online – Codes at a glance, 24 April 2025
11.	OFC000013	Implementing the Online Safety Act: progress update, roadmap illustrative table, 17 October 2024
12.	OFC000014	Illegal Content Judgements Guidance, 16 December 2024 (superseded)
13.	OFC000015	Illegal Content Judgements Guidance, 30 July 2025 (current)
14.	OFC000016	Illegal harms register of risks, 16 December 2024
15.	OFC000017	Illegal harms risk assessment guidance, 16 December 2024
16.	OFC000018	Additional safety measures consultation, 30 June 2025
17.	OFC000019	Proposed Codes for additional measures – Draft Illegal content Codes of Practice for user-to-user services, 30 June 2025
18.	OFC000020	Proposed Codes for additional measures – Draft Protection

		of Children Codes of Practice for user-to-user services, 30 June 2025
19.	OFC000021	Guidance on highly effective age assurance and other Part 5 duties, 16 January 2025
20.	OFC000022	Statement: Age Assurance and Children's Access, 16 January 2025
21.	OFC000023	Children's Risk Assessment Guidance and Children's Risk Profiles, 24 April 2025
22.	OFC000024	Protection of children Code of Practice for user-to-user services, 4 July 2025
23.	OFC000025	Protection of children Code of Practice for search services, 4 July 2025
24.	OFC000026	Update on online safety implementation plans, 30 June 2025
25.	OFC000027	Online Safety Transparency Reporting: Final Transparency Guidance, 21 July 2025
26.	OFC000028	Online Safety Enforcement Guidance, 16 December 2024
27.	OFC000029	Guidance on highly effective age assurance for Part 3 services, 24 April 2025
28.	OFC000030	Online Safety Information Powers Guidance: Guidance for information gathering powers under the Online Safety Act 2023, 26 February 2025