Witness Name: Sarah Connolly
Exhibits: SC/01- SC/42
Dated: 03 September 2025

THE SOUTHPORT INQUIRY

WITNESS STATEMENT OF SARAH CONNOLLY

I, Sarah Connolly, will say as follows: -

Introductory Matters

1. I am the interim Director General for the Digital Technologies and Infrastructure Group within the Department for Science, Innovation and Technology (**DSIT**). I have been in post since 11 August 2025. Previously I was the Director of Digital Infrastructure from January 2024, and prior to that I was the Director of Security and Online Harms from October 2017 to December 2023.

2. This witness statement is made to assist the Southport Inquiry (**the Inquiry**) with the matters set out in the Rule 9 Request dated 8 August 2025.

3. Whilst I have a degree of personal recollection of some of the events or processes described in this witness statement which occurred during my tenure as Director of Security and Online Harms, some events occurred after I had left the team. Where that is the case, I have co-ordinated and consulted with colleagues across DSIT who have direct knowledge and experience of matters covered in this statement. Their contributions have been used to respond to the Rule 9 Request. My statement therefore relies upon those contributions to form the responses in this statement. I have also relied on document archive searches conducted by colleagues.

4. Before providing my statement, I would like to express my deepest sympathy for the families of those killed in the attack, those who were injured and their families, and all whose lives have been affected.

Role and Remit/Responsibilities of DSIT

Creation and Remit of DSIT

5. Prior to February 2023, the Department of Digital, Culture, Media and Sport (**DCMS**) was responsible for a large amount of digital policy across government, including online harms and security, telecommunications and digital infrastructure, digital and tech policy, the cyber and artificial intelligence (**AI**) sectors, and data infrastructure.

6. On 7 February 2023, machinery of government changes were announced which included the creation of DSIT. Following those changes, responsibility for digital policy was transferred from DCMS to DSIT. The formal transfer of responsibilities was completed on 3 May 2023 in accordance with a transfer of functions order[1] **[SC/01]**. **DSIT000005** This statement covers both the work carried out by DCMS up to 7 February 2023 and the work which was subsequently undertaken by DSIT in relation to online safety.

7. DSIT has a wide remit and is responsible for policy including AI, scientific research and development, space, cyber security, digital infrastructure, the Government Digital Service, as well as online safety.

DSIT's Online Safety Responsibilities

8. DSIT has overarching responsibility for online safety policy. This remit is wider than online safety regulation and includes responsibility for policies relating to mis- and disinformation, media literacy and online safety technologies which help to make the online environment safer for all users.

9. Although DSIT has this overarching responsibility, there are specific online policy issues where responsibility is held by other government departments. Most pertinently in this case, policies for online terrorism and extremism are the responsibility of the Home Office (**HO**). That is not unusual or limited to terrorism: policy relating to

---

[1] The Secretaries of State for Energy Security and Net Zero, for Science, Innovation and Technology, for Business and Trade, and for Culture, Media and Sport and the Transfer of Functions (National Security and Investment Act 2021 etc) Order 2023

accessing online educational and social development tools is the responsibility of the Department for Education (**DfE**), policies concerning the mental health and wellbeing of children is the responsibility of the Department of Health and Social Care (**DHSC**) and so on. In such cases, DSIT works closely with other departments on their respective areas of responsibility to ensure we are aligned - across legislative, policy and/or operational measures - to deliver a coherent and responsive approach to online safety.

10. Internet services policy is reserved under all three devolution settlements. Therefore, online safety policy, including child online safety, is primarily a reserved matter, meaning it is overseen by the UK Government, rather than the devolved administrations. However, some aspects of online safety policy such as media literacy (which falls within the remit of education policy) are not reserved and the devolved administrations are responsible for these policies within their respective jurisdictions.

Online Harms and the Online Safety Act 2023

11. The Online Safety Act 2023 ("**the Act**") **[SC/02]** sets out measures to protect children online, and these are enforced by the Office of Communications (**Ofcom**) across the UK. The Act also legislates for a number of new offences (explained in more detail below). The territorial extent of these offences varies and they do not all apply across the whole UK. Devolved administrations implement complementary policies and initiatives. These might include educational programs, local enforcement strategies and community support services. **DSIT000041**

The position before the Online Safety Act 2023

12. Prior to the Act, the regulation of online material was fragmented. Government was reliant upon online platforms having their own measures in place to address content harmful to children, such as terms of service which prevented harmful content being available, and the platforms being consistent in enforcing those terms of service. Government was, therefore, reliant on the industry working in partnership with it to deliver any online safety initiatives.

13. The EU's e-Commerce Directive[2], dated 8 June 2000 and as implemented into domestic law, made consistent the position that providers of platforms were not liable under criminal or civil law for illegal or infringing content they hosted, unless they became aware that it was present on their sites. Where a platform became aware of such content, the e-Commerce Directive mandated that the platform had to act expeditiously to remove it. The directive did not place an obligation on service providers to monitor the content on their platforms. However, it did not completely absolve service providers of responsibility, i.e. a platform could be liable for a criminal offence when it was aware of illegal content and did not act quickly to remove it. Enforcement in such a case, as with criminal offences generally, was a matter for law enforcement and the Crown Prosecution Service, which could bring criminal proceedings against a provider. The e-Commerce Directive stopped applying to the UK after the EU exit transition period, but the UK Government continued to uphold the liability protections.

14. There were a series of legislative and regulatory measures in place prior to the Act, each relating to specific types of online activity and the types of harm that those activities may cause. These measures[3] included:

    a. Data protection law, enforced by the Information Commissioner's Office **(the ICO)**. This included the Data Protection Act 1998, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and, from 2018, GDPR and the Data Protection Act 2018. From 1 January 2021, the UK GDPR applied domestically;

    b. The Electoral Commission had oversight of the activity of political parties, and other campaigners, including activity on social media. The Political Parties, Elections and Referendums Act 2000 provided the Electoral Commission with the powers and functions to regulate political finance in the UK. Electoral law was also enforced by the police, who led on the Representation of the People Act 1983 offences. The Electoral Commission had powers to investigate breaches of the rules to funding

---

[2] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')

[3] From The Online Safety White Paper pages 33 to 34.

and spending for election and referendum campaigns, which included digital campaigning;

c. The Digital Economy Act 2017 provided for the regulation of providers of online commercial pornography to ensure that pornographic material would not normally be accessible by those under 18, and that content which was deemed to be extreme pornographic material was not made available to any user. These provisions were never commenced as they were overtaken by the Online Safety Act;

d. The Equality and Human Rights Commission had oversight of the Equality Act 2010 and the UK application of the European Convention on Human Rights and the Human Rights Act 1998, which incorporated the convention into domestic law. In particular, in this context, this included oversight of the right to freedom of expression under Article 10, which applied to online activity;

e. Ofcom had oversight of video-on-demand services. The EU's Audiovisual Media Services Directive 2010 codified requirements for the UK to regulate editorial content (programming) on UK 'video-on-demand' services. These were implemented as Part 4A of the Communications Act 2003, which made Ofcom the responsible regulator – overseeing compliance on content requirements that covered protecting under 18s, preventing incitement to hate, and commercial references in programmes;

f. The revised EU Audiovisual Media Services Directive 2018, introduced new high-level requirements for video sharing platforms such as YouTube. These requirements were implemented as Part 4B of the Communications Act 2003, for which Ofcom was also responsible. This placed requirements on 'video sharing platforms' to take 'appropriate measures' to protect minors from harmful content, protect the general public from illegal content and content that incited violence and/or hatred, and introduce basic requirements around advertising. Following the UK's withdrawal from the European Union, the directive was transposed into UK law by the Audiovisual Media Services Regulations 2020;

g. The Gambling Commission had responsibility for the licensing and regulation of online gambling under the Gambling Act 2005. DCMS worked with the Commission

to tighten advertising rules on gambling and introduce age verification requirements and launched GAMSTOP, the online self-exclusion scheme;

h. The Competition and Markets Authority (CMA) had responsibility for the enforcement of consumer protection law online.

15. The above examples relate predominantly to regulation of online activity, for example the regulations at a) helped to protect users' personal data, while the regulations at f) helped to regulate the gambling industry and aimed to prevent addiction to online gambling services.

16. However, these regimes were not designed to specifically address harms which could arise from use of social media platforms. The increase in the number and use of social media platforms, plus the speed with which harmful content could reach a large number of users, led government to consider whether regulation was necessary.

17. Three of the four major social media platforms were created in the mid 2000s: Facebook in 2004, Youtube in 2005 and Twitter (now X) in 2006; TikTok was launched later in 2016. Government work on children's online safety began in 2007, when Dr Tanya Byron was commissioned by the Department for Children, Schools and Families, now known as DfE, to examine the harms which children faced from the internet and video games. Her 2008 report **[SC/03]** recommended that the existing Home Secretary's Taskforce on Child Protection on the Internet, was transformed into the UK Council for Child Internet Safety (**UKCCIS**).

DSIT000043

18. UKCCIS was launched in September 2008 and became a group comprising over 200 organisations drawn from across government, industry, academia and civil society organisations, who worked in partnership to keep children safe while online **[SC/04]** and **[SC/05]**. It comprised an executive board, which was chaired by ministers and met on a quarterly basis. The role of the executive board was to identify priority areas of work for UKCCIS and set its strategic direction.

DSIT000044

DSIT000006

19. In addition there were five working groups, each focused on a specific area of interest, such as social media and digital resilience. The secretariat for UKCCIS was provided by DCMS, as overall policy lead for online safety.

The House of Lords Communications Committee Report

20. In 2017 the House of Lords Communications Committee published a report titled **DSIT000019** Growing Up with the Internet [**SC/06**]. Its aim was to understand the challenges, as well as the opportunities, which children faced while interacting with internet technologies. In a summary of their findings, members of the committee expressed the view that when children were online, they should have the same rights and be treated with the same amount of respect and care that had been established in offline settings. The inquiry also found that:

    a. Children's unique needs were not adequately addressed in the online world;

    a. Government responsibility was fragmented, with poor coordination across departments and sectors;

    b. There was an issue of industry self-regulation, which often prioritised commercial interests over child safety;

    c. There was a need for a more unified and proactive approach to safeguarding children's rights online; and

    d. Digital literacy was a vital skill that needs appropriate attention in education.

21. The report made several recommendations, which included:

    a. There should be minimum standards for internet services, including child-friendly design, default-on settings for privacy, and quick responses from social media / content sharing companies to removing upsetting content when reported by children;

    b. That those minimum standards should be captured in a code of conduct for industry compliance, agreed upon in a stakeholder summit;

    c. That irrespective of EU membership, the UK should maintain the standards set by General Data Protection Regulation in respect of children;

d. That digital literacy be integrated into the core educational curriculum, alongside reading, writing, and maths, with mandatory PSHE education to address online risks and responsibilities;

e. The appointment of a Children's Digital Champion within the CO to lead coordinated government action and advocate for children's interests.

The Internet Safety Green Paper, October 2017

22. Driven by growing sense of concern in Parliament, press and the public that harm was occurring online, the UK Government published its Internet Safety Strategy Green Paper in October 2017 (**the Green Paper**) [**SC/07**] and ran a consultation on its contents, which closed in December 2017. **DSIT000020**

23. When preparing the Green Paper, DCMS took into account the House of Lords report referred to at paragraph 20 above and was able to address a number of the **DSIT000008** recommendations [**SC/08**]. Where recommendations were not included within the Green Paper (recommendations 3; 4; 6; 7; 9; 11; 13; 19; 20; 21; 22; 23; 27; 28 and 35), DCMS provided the House of Lords Communications Committee with an explanation as to why.

24. DCMS led the work on the Green Paper and the overall strategy, discussing with other departments with an interest in online safety, including the HO, DHSC and the Ministry of Justice (**MOJ**). The Green Paper set out three key principles which would underpin the government's work in this area:

a. That what was unacceptable offline should be unacceptable online;

b. That all users should be empowered to manage their online risks and stay safe;

c. That technology companies had a responsibility to their users.

25. The consultation questions which accompanied the Green Paper were focused on four main government priorities:

a. Setting out the responsibilities which online content providers had towards their users;

b. Encouraging better technological solutions and their widespread use;

c. Supporting children, parents and carers to improve online safety;

d. Directly tackling a range of online harms.

26. The Green Paper was part of the government's Digital Charter, which had two fundamental aims: to position the UK as the best place to develop and deploy new technology, while at the same time making the UK the safest place to be online in the world.

27. The government response to the Green Paper was published in May 2018 [**SC/09**] **DSIT000018** The response recognised three main issues:

a. That online behaviours too often failed to meet acceptable standards;

b. That users could feel powerless to address those issues;

c. That technology companies were able to operate without proper oversight, transparency or accountability, and that commercial interests meant that those companies could often fail to act in users' best interests.

28. The response set out the Government's view that industry needed to take a more proactive approach to pre-empt potential issues before they arose. Government aimed to adopt a 'safety first' approach, which would build on secure by design principles, to persuade developers and designers to include safety features in new applications and platforms from the outset. Government envisaged establishing new safety baselines for digital platforms and products, working with consumer groups and retailers to agree standards and promote best practice to protect user safety and wellbeing.

29. The consultation responses showed that of the almost 600 received:

a. 296 individuals confirmed that they had witnessed inappropriate or harmful content online;

b. 149 individuals said that they had experienced online abuse. Of these, 130 individuals had experienced insults, 70 harassment, 57 threats, and 51 bullying. 15 individuals said that they experienced the abuse daily and 27 said weekly. 78 individuals said that the abuse related to political or social views. 82 individuals said that they did not know the person/people perpetrating the online abuse;

c. 330 individuals confirmed that they knew how to report potentially illegal or upsetting content on social media, but only 158 individuals had reported this content before; and

d. Only 66 individuals thought that their reported concerns were taken seriously by social media companies.

30. Overall, the responses to the consultation set out a broadly common view of the problems. The message from both users of online services, and representatives of wider civil society replying to the consultation, was that online standards often failed to meet the behaviours set out in social media platforms' terms of service.

31. One of the Green Paper's recommendations was to extend UKCCIS' focus to all online users rather than just children. It also proposed that the UKCCIS executive board be reduced in size, with remaining members being given a higher profile. In the response, government confirmed its intention to evolve UKCCIS into the UK Council for Internet Safety (UKCIS) in 2018 **[SC/10]** **DSIT000016**

32. Upon its creation UKCIS set out a number of strategic goals:

a. A safer online experience for the most vulnerable groups in society;

b. The development of products, platforms and services which were safer by default for all their users;

c. Providing parents, teachers and other professionals with the tools to recognise and respond to online harms;

33. Ensuring a rapid and consistent cross sector response to emerging evidence of harms.

34. It is worth noting that DSIT is currently reviewing the best mechanisms to continue to engage industry and civil society now that the Online Safety Act's illegal and child duties are in force. This work includes reviewing the role of UKCIS.

35. The Green Paper announced that DCMS and HO would work jointly on a White Paper which would set out proposals for future legislation on the full range of online harms, including both illegal and harmful content, covering:

    a. The social media code of practice;

    b. Transparency reporting;

    c. Online advertising;

    d. Age verification tooling;

    e. Policies aimed at improving the mental health of children and young people, including the impact of screen time;

    f. Live streaming issues; and

    g. Work to define harmful content.

The Online Safety White Paper, April 2019

36. In April 2019 government published the Online Safety White Paper (**the White Paper**) **DSIT000038** [**SC/11**], which set out government's intention to establish *"a new regulatory framework to improve our citizens' online safety"*. The objectives of the proposed framework, to be overseen by an independent regulator, were to protect users from the harmful psychological effects of internet services and exposure to illegal content. In particular, it aimed to protect against harmful content directed towards children, including content depicting suicide and self-harm.

37. The White Paper, which was led by DCMS and HO, was based on a range of external evidence sources. The principal sources of data on internet service usage and user harm came from the ICO and Ofcom reports on media use and attitudes. Some key findings from Ofcom's *Children and parents: Media use and attitudes report 2018* ("**the**

DSIT000025

2018 Report") **[SC/12]** regarding the time spent by children online were specifically mentioned in the White Paper: *'Nearly nine in ten UK adults are online and adult users spend around one day a week on the internet. This is also true for children and young people, with 99 per cent of 12-15 year olds going online, spending an average of twenty and a half hours a week on the internet.'* **[SC/11]** DSIT000038

38. The 2018 Report found that children aged 5-15 spent an average of 15 hours and 18 minutes online in a typical school week and weekend. It also provided data on the specific online services which children were using, although this was not specifically mentioned in the White Paper, concluding that the main online activities conducted by children were video streaming, online gaming, and social media:

    a. one third of 3-4 year olds (32 per cent) and half of all 5-15 year olds (49 per cent) said they use "Over The Top television" services like Netflix, Amazon Prime Video and Now TV. YouTube was described as "*increasingly […] the viewing platform of choice*" with close to half of 3-4 year olds (45 per cent) having used it, rising to 89 per cent of 12-15 year olds;

    b. among those who play games, three-quarters of 5-15 year olds play games online. The incidence of online gaming increases with age, ranging from 37 per cent for 3-4 year olds to 87 per cent for 12-15 year olds;

    c. 70 per cent of 12-15 year olds and 20 per cent of 8-11 year olds who go online had a social media profile. Facebook remained the most popular social media site or messaging app, used by 72 per cent of 12-15 year olds with a social media profile **[SC/12]** DSIT000025

39. The White Paper also cited evidence on the growing scale of harmful content and activity that people experience online. It explained that online services could be used to spread terrorist propaganda and child abuse content, a tool for abuse and bullying, and to undermine civil discourse. It referred to the following evidence from the Ofcom and ICO joint 2018 survey of Internet users' experience of harm online: *'Despite the many benefits of the internet, more than one in four adult users in the UK have experienced some form of harm related either to content or interactions online'* **[SC/13]** DSIT000023

40. The White Paper went on to draw on a range of research and reporting from other organisations which detailed the prevalence of harmful content online, including that

specifically linked to children. For example, it highlighted evidence of child sexual exploitation and abuse (**CSEA**) which had been published by the National Center for Missing and Exploited Children and the Internet Watch Foundation. Industry transparency reports were also cited, such as Facebook's 2018 transparency report, which reported removing over 14 million pieces of content related to terrorism or violent extremism in 2018.

41. Nevertheless, the White Paper acknowledged that '*most children have a positive experience online*', finding that children used the internet for social networking and connecting with peers, as well as to access educational resources, information, and entertainment. The White Paper's findings on the benefits to children of internet use included:

    a. A literature review by UKCCIS (2017) which highlighted evidence that young people recognised the positive role of the internet in relation to self-expression, developing understanding, bringing people together and respecting and celebrating differences **[SC/14]** **DSIT000022**

    b. Research by UNICEF (2017) which showed that use of technology was beneficial for children's social relationships, enabling them to enhance existing relationships and build positive friendships online **[SC/15]** **DSIT000046**

    c. A report by The Royal Society for Public Health in 2017 which found that reading blogs or watching vlogs on personal health issues helped young people improve their knowledge and understanding, prompted individuals to access health services and enabled young people to better explain their own health issues or make better choices **[SC/16]**. This report also found that young people were increasingly turning to social media as a means of emotional support to prevent and address mental health issues; **DSIT000042**

    d. The 2018 Report showed that nine in ten social media users aged 12-15 stated that its use has made them feel happy or helped them feel closer to their friends **[SC/12]**. Two thirds of 12-15 year olds who used social media or messaging sites said they sent support messages, comments, or posts to friends if they were having a difficult time. One in eight supported causes or organisations by sharing or commenting on posts. **DSIT000025**

e. A 2019 UK Safer Internet Centre survey, showed that 70 per cent of young people surveyed said that being online helped them understand what was happening in the world, with 60 per cent noting they had only seen or heard about certain issues or news because they heard about them from the internet **[SC/17]**. 43 per cent said **DSIT000045** they had been inspired to take action because of something they saw online, with 48 per cent stating being online made them feel that their voice or actions matter.

The Government Response to the White Paper, 2020

42. On 15 February 2020, DCMS and HO jointly published an interim response to the White Paper to set out initial thinking on a number of areas raised during the **DSIT000037** consultation **[SC/18].** The full response to the White Paper was published on 15 December 2020 [**SC/19**] **DSIT000039**

43. The regulatory regime set out in the White Paper would establish different expectations of content management depending on whether content or activity was illegal or legal but potentially harmful, with different expectations being set depending on whether that potentially harmful content was liable to be seen by children. Regulation would not force companies to remove specific pieces of legal content, but would require them to state what content and behaviour was acceptable on their platforms and enforce this consistently and transparently. Companies would also be required to have adequate redress mechanisms in place to allow users to report harmful content or challenge the removal of content.

44. In relation to industry, government set out that only companies which provide services or had functionality on their sites which facilitated the sharing of user generated content or actions, e.g. through comments, forums or video sharing would fall within the scope of the legislation.

45. On the issue of children's use of online services, government indicated that legislative proposals would expect industry to use a proportionate range of tools, including age assurance and age verification technologies, to prevent children from accessing age inappropriate material.

46. The legislation would apply to search engines, as well as companies whose services:

a. Hosted user-generated content which could be accessed by UK users; and/or

b. Facilitated public or private interaction between users, one or more of whom is within the UK.

47. In order to protect journalistic freedoms, content published by a news provider would fall outside the legislation, as would any comments on those sites.

48. It was confirmed that the legislation would set out a definition of harmful content and activity, and that the companies within the scope of the legislation would have a duty of care towards users. It would be for Ofcom to issue Codes of Practice to outline the systems and processes which would need to be adopted in order to meet that duty. Expectations on those companies would depend upon the type of content on their platforms. Content would be categorised in three ways: illegal content, content which was harmful to children and content which could legally be accessed by adults, but which may be harmful to them.

49. The proposed legislation would also take a tiered approach to different types of services with additional duties on Category 1 services (see paragraph 96 for category thresholds). Services which had large audiences and increased functionality to share material were likely to fall within Category 1 (large user-to-user services). The thresholds for determining whether a service would fall into Category 1 would be included in the legislation. It was thought that the majority of online services would fall within Category 2 (large search services) and companies providing those services would be expected address illegal content and activity and take proportionate steps to protect children. High risk, high reach services would fall within Category 1 and providers of those services would be required to take additional steps in relation to content which was legal but potentially harmful to adults.

Wider concepts

50. It may be helpful at this stage to set out some of the key considerations which need to be balanced during the creation of the policy and the passage of what became the Online Safety Act 2023.

51. The most significant issue was the balance between the risk of illegal and, particularly, harmful material found online; and maintaining the right of freedom of expression.

There was significant pressure on Ministers from the public and press to remove content which was deemed 'harmful' (or sometimes 'legal but harmful'), but which was not in itself illegal. In cases where that material might have been seen by children, the case was fairly straightforward that robust protections should be put in place. In the case for adults, it was less clear. In some cases vulnerable adults, such as, for example those with serious mental health problems, may be at risk if they were to be pushed content which promoted self-harm or suicide, but which does not reach a criminal threshold. There are strongly held views on both sides of the debate: on the one side that such content should be removed from all platforms in order to prevent individuals from harm; on the other than if material has not be determined by Parliament to be illegal then any removal of it is a violation of freedom of expression.

52. More widely, government was concerned to encourage innovation and investment economic growth in the digital sector. The digital sector is one of the fastest growing sectors of the economy, employing over 1.7 million people in 2024 with an estimated economic contribution of £153.5 billion Gross Value Added (GVA) to the UK in 2023[4]. As such, government wanted to regulate the sector in a way which was proportionate, supported growth and encouraged innovation to tackle the challenges.

53. The details of the regulatory system were inherently contentious – and the final position is set out below – but two issues caused particular debate. The first, is the degree to which particular services or sectors, notably the press and small and medium sized enterprises (SMEs), were in scope of the regulator. Concerns were consistently raised about ensuring that the regulation was proportionate and targeted, while tackling a wide variety of harms. The second, is the usage of age assurance tools to prevent under 18s accessing material inappropriate for children, notably pornography. There was significant concern to ensure that the regulations enabled the goal without either requiring children to provide data or websites storing data about adults' preferences without strong protections in place.

54. The approach taken by government was for the Act to impose broad duties on companies covered by the legislation, with powers given to Ofcom to independently regulate. Powers which were given to Ofcom included: a requirement to develop and produce Codes of Practice and guidance setting out how companies could fulfil those

---

[4] Figures from DSIT Economic Estimates

duties; the ability to monitor companies' compliance with the duties; and the ability to take enforcement action, including sizable fines, against companies who were in breach. As mentioned above, DSIT has a broader responsibility for policy and this includes setting strategic priorities for Ofcom.

55. DSIT and Ofcom worked together, and continue to do so, pursuant to formal memorandums of understanding, joint steering or governance groups, and regular bilateral meetings to coordinate the implementation and evaluation of the Act and stakeholder engagement. Where this work involved policy areas led by other departments (such as terrorism), those departments worked alongside DSIT and Ofcom to determine how the Act would regard those particular policy areas within the wider framework.

The Online Safety Bill

56. The government response to the White Paper announced the government's intention to bring forward the Online Safety Bill **("the Bill")** in 2021. DCMS worked on an impact assessment for the Bill, which it published in draft on 27 January 2021 **[SC/20]**. The **DSIT000009** **DSIT000010** draft Bill **[SC/21]** went through pre-legislative scrutiny by a joint committee, made up of both MPs and peers, which published its report in December 2021 **[SC/22]**. The **DSIT000021** report specifically highlighted that algorithms played a part in what people experience online, which risked increased exposure to and the amplification of harmful content. It identified that children were at most risk of such harm and that often online services were not designed with children in mind. The committee made a series of recommendations, which it felt would hold service providers liable for the risks that result from the design and operation of their platforms, while protecting freedom of speech. The committee highlighted that it had several concerns with the Bill, including a lack of clarity about what type of content would be prioritised under the Bill's safety duties, which service providers would fall within Category 1, that the provisions concerning adult access to harmful content could have a chilling effect on the right to freedom of expression, that transparency requirements on platforms may not go far enough, that Ofcom's powers may be insufficient and that there was insufficient protection for children.

57. In March 2022, the government produced its response to the committee's report **DSIT000017** **[SC/23].** In that response, government agreed with some of the committee's recommendations, including setting out details of what would be a priority offence

within the Bill, such as terrorism or child sexual exploitation and abuse (see paragraph 77) and to protect children by restricting access to pornography on all sites, rather than just on user-to-user services. The Bill was introduced in the House of Commons in March 2022 and was subject to extensive legislative scrutiny from both Houses.

58. On 28 November 2022, following a change in Prime Minister and during the Bill's passage, government announced plans to make amendments to the Bill, which included the removal of the legal but harmful provisions relating to adults. Under the original version of the Bill, Category 1 platforms (large user-to-user services, see paragraph 96) would have been required to conduct risk assessments in relation to harmful material which could be accessed by adults (see paragraphs 75-83 for categorisation of material). Platforms were also required to be clear in their terms of service how they could treat legal content that could be harmful to adults, such as taking such content down, restricting access, or limiting its promotion. These provisions were replaced by the introduction of transparency, accountability and free speech duties, which included a requirement for Category 1 Services to set out what content they ban or restrict access to and what activity would result in a ban or suspension for their users. The Bill set out requirements for systems and processes to be in place to enforce those terms and ensure platforms didn't remove content beyond this. User redress duties were introduced in relation to the flagging of banned content, over-removal of content and non-compliance with duties. The user empowerment duties on Category 1 Services were retained, but with a new list of 'relevant content' set out on the face of the Bill, rather than 'content that is harmful to adults'. This shift aimed to uphold freedom of expression while ensuring platforms maintained transparency and accountability in managing user content.

59. The government made a large number of additional amendments to the Bill during parliamentary passage, including bringing in a limited form of senior management liability for tech executives to be used in specific circumstances, adding specific references to services' functionalities and adding a clause at the start of the Act to summarise its aims and intent. Successful amendments were also made in the House of Lords with the aim of bringing small but risky services into scope of categorisation.

60. The Bill gained Royal Assent on 26 October 2023, becoming the Online Safety Act **DSIT000041** 2023 **[SC/02].** DCMS and subsequently DSIT's attention then turned to implementation.

The Online Safety Act, 2023

61. The Act imposes a range of new duties on social media companies (user-to-user services) and search services (sometimes referred to as Part 3 providers), and providers of internet services on which provider pornographic content is published or displayed (sometimes referred to as Part 5 providers), making them more responsible for their users' safety on their platforms. Providers need to implement systems and processes to reduce risks their services are used for illegal activity, and to take down illegal content when it does appear.

62. Under the Act, all regulated user-to-user services, search services or combined services are required to tackle illegal content and, if their service is likely to be accessed by children, protect children from harmful content. Category 1 (large user-to-user services, Category 2A (large search services) and Category 2B (other categorised user-to-user services) will have additional duties; all have additional duties on transparency reporting and policies relating to disclosure of information about use of service by deceased child users. Category 2A additionally have enhanced requirements on risk assessments and record keeping, as well as fraudulent advertising duties.

DSIT000040

63. As set out in the Act's explanatory notes **[SC/24],** the legislation requires providers of regulated user-to-user and search services to:

    a. Assess the risks of harm to those users present on the service;

    b. Take steps to mitigate and manage the risks of harm to individuals arising from illegal content and activity, and (for services likely to be accessed by children) content and activity that is harmful to children. Providers will also need to assess the risk of their services being used for the commission or facilitation of a priority offence and to design and operate their services to mitigate this risk;

    c. Put in place systems and processes which allow users and affected persons to report specified types of content and activity to the service provider;

    d. Establish a transparent and easy to use complaints procedure which allows for complaints of specified types to be made;

e. Have particular regard to the importance of protecting users' legal rights to freedom of expression and protecting users from a breach of a legal right to privacy when implementing safety policies and procedures; and

f. Put in place systems and processes designed to ensure that detected but unreported CSEA content is reported to the National Crime Agency.

64. User-to-user services which fall into Category 1 are subject to additional legal requirements, including to:

a. Improve transparency and accountability and protect free speech. Those user-to-user services which meet the Category 1 threshold conditions must have systems and processes to ensure they only remove or restrict access to content, or ban or suspend users, where allowed by their terms of service, or where they otherwise have a legal obligation to do so;

b. Carry out an assessment of the impact that safety policies and procedures will have on users' legal rights to freedom of expression, including on access to and treatment of news publisher and journalistic content, and users' privacy, and demonstrate the steps they have taken to mitigate any impact;

c. Specify in a public statement the steps taken to protect users' legal rights to freedom of expression and users' privacy;

d. Put in place systems and processes designed to ensure that the importance of the free expression of content of democratic importance is taken into account when making decisions about how to treat such content;

e. Put in place systems and processes designed to ensure that the importance of the free expression of journalistic content is considered when making decisions about how to treat such content;

f. Notify and offer a right of appeal to a recognised news publisher before removing or moderating its content, or taking action against its account;

g. Put in place a dedicated and expedited complaints procedure that ensures that the decisions of the service provider to take action against a user because of a particular piece of journalistic content can be challenged;

h. Offer optional user verification and user empowerment tools to adults on their sites; and proactively ask their registered adult users at the first possible opportunity how they would like the user empowerment content tools to be applied; and

i. Put in place proportionate systems and processes to prevent the risk of users encountering fraudulent adverts.

65. Those search services which meet the Category 2A threshold conditions are under a duty to produce annual transparency reports and put in place proportionate systems and processes to prevent the risk of users encountering fraudulent adverts.

66. Category 1, 2A, and 2B Services are also under duties to set out their policies on disclosing information to the parents of deceased child users, provide details about this in the terms of service or a publicly available statement, and operate a complaints procedure in relation to these duties.

67. The Act also requires providers of internet services which make pornographic material available by way of the service (as opposed to enabling users to generate or share such content) to use age verification or age estimation (or both), to ensure that children are not normally able to encounter that pornographic content.

68. The Act creates a false communications offence and a threatening communications offence. It also amends the existing communications offences in the Malicious Communications Act 1988, Malicious Communications (Northern Ireland) Order 1988, and Section 127 of the Communications Act 2003 to reflect this. It creates a new "cyberflashing" offence, an offence of sending or showing flashing images electronically to people with epilepsy, and an offence of encouraging or assisting serious self-harm. It also inserts new intimate image abuse offences to the Sexual Offences Act 2003.

69. The Act confers new powers on Ofcom to require regulated user-to-user and search services to use accredited technology to deal with CSEA and terrorism content, or

make best endeavours to develop or source technology to deal with CSEA content, where necessary and proportionate.

70. The new powers conferred on Ofcom also include the power to give enforcement notifications (which may set out the steps required to remedy a contravention) and the power to impose financial penalties of up to £18 million or 10% of qualifying worldwide revenue, whichever is greater. Ofcom can also, in certain circumstances, apply to the Courts for an order imposing business disruption measures on a provider.

71. The Act requires Ofcom to produce Codes of Practice for service providers, setting out the recommended steps that providers can take in order to comply with the legal requirements described above. A provider may take different measures to those recommended in the Codes of Practice. A provider will be treated as having complied with the relevant legal obligation if the provider takes the steps recommended in the relevant code of practice for complying with that obligation.

72. In crises posing a threat to public safety, public health or national security, the Secretary of State can give directions to Ofcom under section 175 of the Act. Under this provision Ofcom can be required to prioritise specific objectives for a defined period of time in its use of its media literacy powers in order to address a specific threat or to require providers to make public information about how they have responded to the threat.

73. The Act includes protections which have been designed specifically for children. Providers of user-to-user and search services that are likely to be accessed by children need to take steps to protect children from harmful content and behaviour, and these duties came into effect on 25 July 2025. For example, in-scope platforms are required to have in place measures, such as age assurance tools, to prevent children from accessing harmful and age-inappropriate content, and to provide parents and children with clear and accessible ways to report problems online when they do arise.

74. Many of the duties in the Act are supplemented by Codes of Practice issued by Ofcom. While the Act sets out those duties and what providers must do at a high level, the Codes of Practice provide more detailed provisions, including measures for different types and sizes of service, which set out the concrete steps which providers can take to ensure compliance with the duties. As a provider that follows all the relevant steps in a code of practice is considered to have complied with the corresponding duties, the

codes provide a degree of certainty beyond the duties themselves. During passage this was considered especially important given the large number of providers of smaller services regulated by the Act, which may lack the resources for detailed consideration of what measures would be proportionate for their services.

Categorisations of Content

i) Illegal Content

75. Illegal content is content that "amounts to a relevant offence". The Act sets this out at section 59, including the ways in which content consisting of words, images, speech or sound might "amount to" an offence:

i. Where the use of the words, images, speech or sound is an offence.

For example, section 4 of the Public Order Act 1986 makes it an offence to use threatening, abusive or insulting words towards another person with intent to cause that person to believe that immediate unlawful violence will be used against them or another person. Content comprising or containing threatening words which were intended to make the person they were directed towards believe that immediate unlawful violence would be used against a person would therefore amount to this offence and be illegal content;

ii. Where the possession, viewing or accessing of the content is an offence;

For example, section 63 of the Criminal Justice and Immigration Act 2008 makes possession of an extreme pornographic image an offence. Content that met the definition of an "extreme pornographic image" would therefore amount to the offence and be illegal content;

iii. Where the publication or dissemination of the content constitutes a relevant offence.

For example, an offence is committed under section 2 of the Terrorism Act 2006 where a person distributes or circulates a terrorist publication with certain intention or recklessness. Therefore, content that met the definition of a terrorist publication

which was posted with the relevant intention or recklessness would amount to this offence and be illegal content.

76. However, content merely depicting an offence does not amount to an offence (unless the depiction is also an offence). Therefore, a video of a person being violently attacked will not necessarily be illegal content, even where the attack itself is clearly a criminal offence. This aligns with the principle that adults should only be prevented from seeing content where it is illegal (and would also therefore be treated as such in the "offline" world). It is also one of the ways in which the Act protects freedom of expression, especially in relation to journalism and other information which may be especially important in a democratic society.

77. The Act has three schedules which set out "priority offences": Schedule 5 lists terrorism offences, Schedule 6 lists child sexual exploitation and abuse offences and Schedule 7 lists other priority offences. Content which amounts to an offence listed in any of these schedules is "priority illegal content" and particular duties apply in relation to it.

78. Separately from the regulatory regime, Part 10 of the Act created several new communications offences. These are treated in the same way as any other offence under the regulatory regime: content amounting to them will be illegal content and the illegal content duties will apply.

ii) Legal but Harmful Content

79. In Sections 61 and 62, The Act sets out categories of harmful content that platforms and internet search engines need to protect children from encountering. In addition to these specified types of content, providers must also assess for and mitigate risks from "non-designated" content that is harmful to children. The Act sets out a definition for determining whether content falls in this category. DSIT has also published an online explainer, setting out the key features of the Act and how it will address particular types of harmful content, **[SC/25]**, along with an additional impact assessment **[SC/26]**..
DSIT000014 **DSIT000013**

80. The Act does not describe content as 'legal but harmful'. This is a phrase which during the passage of the Act, and still, is often used to describe content which, while not illegal, is capable of causing significant harm. Examples include content which promotes self-harm, suicide or eating disorders, all legal pornography where it is being viewed by children, some legal pornography where it is being viewed by adults and

material promoting dangerous stunts or substance abuse. The duty of care which service providers owe to users differs depending upon whether they are adults or children.

81. For the purposes of the Act, a child is defined as someone who is under the age of 18. Under Section 12 of the Act, adults are able to view legal but harmful content, while service providers which are likely to be accessed by children are under a duty to protect children from such content. The Act will require 'Category 1' services to offer user empowerment tools to adult users to choose whether or not to engage with content that encourages, promotes or provides instructions for suicide, self-harm and eating disorders, and content that is abusive, or incites hate, on the basis of race, religion, sex, sexual orientation, gender reassignment or disability. If applied, these tools will reduce the likelihood that adult users are exposed to these certain categories of content or will alert them to the nature of it. In addition, adult users of Category 1 services will have the ability to verify their identity and access tools which enable them to reduce the likelihood that they see content from non-verified users, and prevent non-verified users from interacting with their content.

iii) Primary Priority and Priority Content

82. Under Section 12 of the Act platforms must use proportionate systems and processes to prevent all children from accessing 'primary priority content', which is pornography or content which encourages, promotes, or provides instructions for either self-harm, suicide or eating disorders. There is a second category of content, known as 'priority content', where platforms must use proportionate systems and processes to ensure that access is age appropriate. 'Priority content' is content which is bullying, abusive or hateful or depicts real or realistic serious violence against a person, real or realistic serious injury of a person in graphic detail, or encourages dangerous stunts or challenges or which encourages the ingestion, inhalation or exposure to harmful substances.

iv) News Publisher Content

83. 'News publisher content' is content either generated directly on a service by a recognised news publisher, content originally published by a recognised news publisher which is uploaded or shared by a user in full (and not edited or clipped) or links to this type of content. A "recognised news publisher" is an entity which meets

the definition at section 56 of the Act. The way in which the types of content are defined means that content which is news publisher content cannot be illegal content or content that's harmful to children, meaning the illegal content and children's safety duties don't apply to it. The Act also contains a provision (as yet un-commenced) requiring Category 1 services to apply protections to news publisher content which requires them to take certain procedural steps before such content is taken down.

Assessment of Content

84. Whether content is treated as being in one category or another will depend not only on the material itself, but also the context in which the content is shared or presented and other information available to the provider. The provider of the service is primarily responsible for assessing whether content is illegal content, content harmful to children or another kind of content. Ofcom can assess whether the provider has followed the correct approach in making this assessment, when deciding whether the provider has complied with its duties. However, it is not expected to reach a definitive conclusion on each piece of material nor substitute its own judgement where the provider has reached a different reasonable conclusion while following the correct approach.

85. The approach that the provider should follow is set out in the Act and expanded on in guidance issued by Ofcom on 16 December 2024. The provider should make a decision on the basis of all the evidence reasonably available to it. Where a provider is assessing whether content is illegal content, it should, on the basis of this evidence, decide if there are reasonable grounds to infer that all elements of the offence, including mental elements such as intention, are present or satisfied. The provider can conclude that such grounds exist on the basis of the content itself, surrounding content or other context or any other evidence reasonably available. If the provider has reasonable grounds to infer that there is a defence that could be used successfully, it should not consider the content illegal content.

86. Therefore, the same material might well be treated differently in different contexts. News footage could be news publisher content when generated on a social media service by the BBC and remain news publisher content when shared in full by another user. In neither instance would the Act's duties require action from the provider. If a part of the footage depicting serious violence were clipped and shared by a user on a service likely to be accessed by children, it would be (priority) content harmful to children, and that service's systems and processes should protect children from

encountering it. If such a clip were shared in a way or a context from which it was reasonable to infer that the person sharing it intended to stir up hatred, for example on the grounds of a certain characteristic, the content would be (priority) illegal content and the service's systems and processes should take it down.

87. Given the type of judgement involved there may be circumstances in which one person may reasonably consider content illegal and another may, also reasonably, consider that content not to be illegal content. Ofcom would not adjudicate which assessment was correct, and the Act does not require that a definitive answer is reached. Instead, if Ofcom were investigating a provider, it could consider whether the systems and processes that provider had in place to comply with the illegal content duties included following the right approach to assessing whether content was illegal.

88. The Act does not displace the role of law enforcement and the CPS in bringing criminal proceedings where a user commits an offence by posting a specific piece of content. Law enforcement does not rely on the Act or any judgement made under it, but takes place independently of it on the basis of specific criminal offences. These parallel approaches allow the criminal justice system to address some of the most serious individual online offences, while the Act seeks to address illegal content efficiently and at scale.

Age Assurance Tools

89. Under the Act, platforms which host primary priority content which is legal, but harmful to children must use highly effective age assurance to prevent children accessing this content. Platforms which allow any form of primary priority content are therefore required to have highly effective age assurance tools in place. Those age assurance tools could be in the form of software which analyses the face of a user and estimates their age, asking for and checking photo ID or using age information from credit card providers or mobile phone networks e.g, asking for and checking photo ID or using age information from credit card providers or mobile phone networks. Ofcom sets out what could constitute highly effective age assurance in guidance which can evolve as technology and evidence develops.

Implementation of the Act

90. The legislation provided for a phased introduction of the Act's provisions and on 26 October 2023 Ofcom produced a document which set out the timeframes for implementation **[SC/27].** Section 43(11) of the Act places a statutory requirement on Ofcom to submit certain draft codes of practice to the Secretary of State with the period of 18 months, beginning with the day on which the Act passed. This requirement ensured that Ofcom prioritised implementation of the illegal content duties, child safety duties. Section 194 also places requirements on Ofcom to publish guidance within the same timeframe. This includes guidance which relates to the same safety duties, as well as separate duties relating to pornography providers, and guidance on enforcement. This deadline has now passed and Ofcom met its statutory obligations.

DSIT000036

91. While DSIT and HO are responsible for bringing the Act's duties into force, many of these do not have full effect until Ofcom has issued the relevant code of practice. The Act applies to over 100,000 online services and priority has been given to the implementation of the provisions relating to illegal content and child safety. Although the illegal content safety duties and children's safety duties were brought into force on 10 January 2024 (along with other provisions), they did not have much practical effect at that time. This is because at that point there were no Codes of Practice relating to those duties, so no providers were obliged to comply with them.

92. The process for issuing a code of practice is set out in the Act and necessarily cannot be done instantly. Ofcom is required under section 41 of the Act to consult with multiple different stakeholders and must comply with certain provisions about the content of the codes. This has, inevitably, taken time, especially as this is a complex area to regulate and requires the careful production of effective Codes of Practice.

93. Under section 43 of the Act, following a consultation on any given code, Ofcom must, after considering all the evidence received, prepare a draft code of practice, which must then be laid before Parliament by the Secretary of State (unless a direction is issued in particular circumstances; so far none have). It is not until a 'praying' period of 40 days (not including any recesses), during which Parliament may object, has passed that Ofcom is able to issue a code of practice. A code of practice then comes into force 21 days after it is made. It is not until this point, in relation to the first code of practice for each duty, that the duty applies to providers and Ofcom is able to assess compliance and take enforcement action where a provider is failing to comply.

94. The draft illegal harms codes was laid in Parliament on 16 December 2024, coming into force on 17 March 2025. Consequently, Ofcom can start enforcing the Illegal Harms Code where it believes platforms have failed to comply and has already begun to enforce these duties. For example, in April 2025 Ofcom launched an investigation into a suicide discussion forum service, which it suspects may have breached the illegal content duties. This investigation is still ongoing.

95. Under the Act, Ofcom was required to undertake research in order to provide advice to the Secretary of State on the appropriate threshold conditions for Category 1, 2A and 2B. Ofcom recommended, in advice published on 25 March 2024 **[SC/28]**, two DSIT000024 different criteria for Category 1, and one criterion each for Category 2A and 2B, based on research undertaken on user numbers, functionalities and any other factors or characteristics considered relevant.

96. For a provider to fall within Category 1, Ofcom recommended that a service be a regulated user-to-user service which has in excess of an average of 34 million UK users per month and uses a content recommender system; or have in excess of 7 million active UK users on average per month, uses a content recommender system and allow users to forward or share user generated content on that service with other users. Category 2A was recommended to apply to search engines which have on average more than 7 million active UK users per month and is not a search engine which only allows a user to search selected sites or databases in relation to a specific theme, topic or genre, such as a price comparison or job-listing service, also known as a 'vertical search service'[5]. For Category 2B, Ofcom recommended that the conditions be met by regulated user-to-user services that have an average number of monthly active UK users that exceeds 3 million and allows users to send direct messages.

97. The regulations[6] were laid in Parliament in December last year in line with Ofcom's advice and came into force on 27 February 2025. Ofcom is now required to assess services and determine which services are categorised, based on the relevant conditions, and publish their determinations on a public register.

98. In addition to publishing guidance alongside the codes on identifying content in the primary priority and priority content categories, which are mentioned above, Ofcom's

---

[6] https://www.legislation.gov.uk/ukdsi/2025/9780348267174

codes also include types of content which could meet the definition of harmful non-designated content, which is legal but potentially harmful content which is not formally referred to in the Act or has been designated as harmful by the Secretary of State. This is to help platforms understand their duties and comply with the Act's requirements.

99. Ofcom published its protection of children consultation in May 2024, which closed in July 2024. Ofcom published its finalised children's access assessments guidance on DSIT000027 16 January 2025 **[SC/29]**, following which services had three months to complete the children's access assessment process. Ofcom has since finalised its Protection of Children Codes, which were laid in Parliament by the Secretary of State on 24 April DSIT000035 2025 **[SC/30]**. Services likely to be accessed by children had until 24 July 2025 to complete a children's risk assessment, to evaluate the risk of harmful content to children on their platforms. Parliament approved the draft Protection of Children codes and on 4 July 2025 Ofcom issued a Protection of Children Code of Practice for user-DSIT000034 to-user services [**SC/31**] and a Protection of Children Code of Practice for search DSIT000033 services [**SC/32**]. Both Codes of Practice suggested measures which service providers should consider adopting, for example age assurance tools, and came into force on 25 July 2025, meaning that the child safety regime is now fully in effect. Ofcom is actively enforcing the duties, and has a number of active investigations into suspected breaches of duties to prevent the sharing of CSEA material and access to pornography. Collectively, the services under investigation have over 9 million unique monthly UK visitors.

100. The next steps to implement the Act include the implementation of the super complaints regime, which will happen at the end of 2025 and the introduction of the fee regime for the financial year 2026/27. The super complaints regime is a mechanism introduced under the Act that allows eligible organisations (not individuals) to raise concerns about systemic issues with regulated services directly with Ofcom. Ofcom is also due to consult on the additional duties for categorised services such as the duty for Category 1 services to adhere to their own terms of service. On 30 June, Ofcom published a consultation to strengthen its Codes of Practice for providers of online services to further improve protections for children and tackle the spread of illegal content **[SC/33]** DSIT000026

Specific questions posed by the Inquiry

Access to content showing a stabbing

101. The Inquiry has made DSIT aware that, prior to the events on 29 July 2024, the perpetrator may have accessed videos via social media which depicted a stabbing. I understand that the content which the Inquiry is referring to is a video of the stabbing of an Australian bishop, which I understand the Inquiry Chair referred to in his opening statement. I am asked if this material should have been available to the perpetrator as at 2021, July 2024 and now.

102. The first matter to consider is whether this material should be classified as being illegal. As a policy department, it is not DSIT's role to assess whether individual pieces of content are illegal. Ofcom, in enforcing the Act, is required to consider whether the correct approach has been followed to determining whether content is illegal content, rather than whether the "correct" conclusion has been reached in any particular case. It is for the social media platform, not DSIT, to decide whether the content is a breach of its own terms of service, and therefore what action (if any) it should take. In some cases, leaving illegal content up on a platform could make the provider liable for a criminal offence. Where this is the case, it will be a matter for the police and CPS to consider bringing a prosecution.

103. Assessing whether or not a particular video amounts to illegal content will depend on the information available to a provider, including contextual information of the type I have described above. It is possible that different providers may make different assessments of whether there are reasonable grounds to infer that all elements of an offence are present. There will often not be a definitive answer about whether content in a particular context is illegal content or not, although some judgements will be more straightforward than others. In this instance, I understand that the social media platform found that the content did not breach its terms of service, from which I infer that it concluded that it was not illegal.

104. As at 29 July 2024, Ofcom's illegal content codes and child safety codes had not come into force. Therefore the Act would not have applied to any services on which the perpetrator viewed content before the incident took place. The decision as to whether that content should have been available online to both adults and children was therefore one for social media platforms to take, in line with their terms of service.

105. Ofcom's illegal content codes came into force on 17 March 2025 [**SC/34** DSIT000030 DSIT000031] [**SC/35**] and on 25 July 2025 the child safety codes also came into force [**SC/31** DSIT000034 DSIT000033] [**SC/32**]. The position now would therefore be different and would vary depending on whether an adult or a child were using the service.

Access by an Adult

106. In relation to an adult, if the content is illegal, the social media company must have in place systems and processes to mitigate the risks of users encountering that material and remove it swiftly once they become aware of its existence on their platform. The provider of the service is primarily responsible for assessing whether content is illegal content, although Ofcom can assess whether the provider has followed the correct approach in making this assessment. The provider should consider all the evidence reasonably available and, on the basis of this evidence, decide if there are reasonable grounds to infer that all elements of the offence, including mental elements, are present or satisfied.

107. If the content is not illegal, but has potential to cause harm, the illegal content duties do not apply and it is for the platform to determine whether the content is in breach of their terms of service and if it is, what action should be taken. This is because The Online Safety Act does not set out to prevent adults from seeking out legal content, nor does it decide what legal content companies should or should not allow on their platforms. Just as adults have freedom in the offline world to make choices around their own consumption of legal products which may be harmful to their health (such as alcohol or tobacco), the Act mirrors this approach by affording them the same freedom to navigate the online world, where this relates to legal content.

Access by a Child

108. The position is now different in relation to a child trying to access that material. Under the child safety duties, services likely to be accessed by children must take proportionate measures to protect children from encountering harmful content, even where this content is not illegal.

109. The child safety duties are such that a service which is likely to be accessed by children must apply age assurance measures and only allow access to the harmful

material where it has sufficient confidence that the user is an adult. It is for Ofcom to assess whether the measures comply with the child safety codes.

Violent and Terrorist Content seen by the Perpetrator

110. The Inquiry has also made DSIT aware that the perpetrator accessed online terrorist material and a range of online material relating to violence and depicting serious injury or death. In relation to online terrorist materials, although DSIT has overarching responsibility for online safety, this is a specific HO policy area and they will be able to provide a response on the policy steps which have been taken to ensure that this type of material is not available online.

111. On 29 July 2024, the intermediary liability regime, which was derived from the e-Commerce Directive (see paragraph 13) was in place, as the relevant parts of the Act had not yet been implemented. If the content which the perpetrator accessed was illegal and its existence had been brought to the platform's attention, the platform would be liable if it did not remove it expeditiously. If the content was not illegal, it would have been for the individual platform to assess the content and decide whether it amounted to a breach of its terms of service, as set out at paragraph 104 above. The current position in relation to this content, following implementation of the Act is set out in paragraph 106 above.

112. In relation to any non-terrorist violent material which the perpetrator accessed prior to the incident, the position would be the same as that set out in paragraphs 13 and 104 above: the relevant provisions of the Act had not come into force and the decision as to whether the material should be available would have been one for the relevant platform or platforms. As to the position should someone try and access such violent content now, the position would be as set out in paragraphs 79 to 81 above.

The Statement of Strategic Priorities

113. In November 2024 DSIT published a draft Statement of Strategic Priorities for Ofcom on online safety **(SSP),** which it consulted on with various stakeholders until 10 January 2025 **[SC/36].** A further draft statement was published in May 2025 **[SC/37]** with the final SSP being published on 2 July 2025 **[SC/38].**

DSIT000011 **DSIT000015** **DSIT000012**

114. The purpose of the SSP was to set out the government's areas of focus for online safety. Ofcom, as the regulator, has to have regard to those priorities as the Act continues to be implemented. In the SSP, DSIT set out its intention to work on the priorities alongside Ofcom. The SSP sets out five priorities:

a. Implementing safety by design, to prevent more harm from occurring in future;

b. Increasing the transparency and accountability of platforms;

c. Maintaining regulatory agility so that it can keep pace with changing technology and behaviour;

d. Building an inclusive and resilient society of well-informed online users; and

e. Supporting continued innovation in safety technologies.

115. Within these five priorities the SSP explicitly mentions harms which are expected to be tackled by Ofcom's work on these priorities. For example, under the 'safety by design' priority the SSP lists terrorism and child sexual exploitation and abuse as areas which it expects platforms to take proactive steps to tackle. The harms set out in the SSP are examples of the priority offences included in the Act, even though not all of them are listed within the SSP. Therefore, the offences of provoking unlawful violence and putting people in fear of violence are ones which DSIT expects Ofcom to tackle through its regulatory work, alongside those explicitly mentioned within the SSP. The SSP was drafted with the intention of helping Ofcom to understand the government's online safety priorities, encouraging the use of the Act's existing powers in ways which DSIT considers to be the most impactful. However, where it becomes clear that some issues cannot be resolved without additional legislation, this is something which government will consider.

116. The SSP specifically highlights, in the section concerning safety by design, that content promoting acts of serious violence, peddling hatred and inciting acts of self harm or suicide are far too easily accessible by users who wish to be or should be protected from such content, especially children. Government makes it clear in the SSP that part of the safety by design priority includes providers looking at all areas of their services and business models, including algorithms and other functionalities when considering how to protect their users. The focus should not just be on the

management of risks, but on the embedding of safety outcomes throughout the design of new features or functions, while considering how to make existing features safer.

117. The Southport attack raised, among other issues, questions about the access that children and violence-fixated individuals have to violent and terrorist materials online. Increasing protections for children on the internet was already a key priority for DSIT and I have described above the measures that have been and are being put in place to improve safety. While the SSP was not drafted with this incident or perpetrator in mind, the priorities that it contains are salient: in particular, the use of safety by design principles to prevent content promoting acts of serious violence online.

118. In terms of non-ideological violence and violence fixated individuals, overall policy responsibility for this area sits with the Home Office. DSIT has been working closely with the Home Office to consider additional measures to tackle the online elements of this issue. As part of their journey to violence, these individuals may consume a mix of legal and illegal content online – some of it explicitly focused on violence but some of it focused on social themes or specific world events.

119. Some of these types of content are already illegal content under the Act (for example, content which intentionally incites violence) or priority content for children (for example, content which depicts or encourages serious violence or injury for which platforms must provide children with 'age appropriate' protection). Some types of content (for example, news reporting about world events) are legal and un-problematic in themselves but may form part of an individual's pathway to violence. The challenge remains that there is no single type of content which pushes individuals towards violence, and therefore it is DSIT's view that using the Act to stop users – particularly children – being exposed by a range of harmful content is the right overarching approach. We will continue to consider the case for amending or strengthening the Act as needed, as well as the case for additional stand-alone powers. Decisions on those matters will, ultimately, be for government ministers and Parliament.

120. On 25 July 2025, Ofcom produced an initial statement to explain how it will work **DSIT000032** within the parameters set by the SSP [**SC/39**]. Under the Act it is obliged to report annually going forward on the work it has done to meet the aims set out in the SSP.

Use of VPNs

121. The Inquiry has asked about the use of virtual private networks (VPNs). A VPN creates a secure encrypted link between a user's device and the internet. This means that the user's data is scrambled and cannot be seen by the service provider. VPNs are legal tools with many legitimate uses. They are often used to enable users to stay secure when using public wi-fi services, which are often unsecured, or to protect privacy. However they can also be used as a way of bypassing geographical restrictions on accessing certain data, for example the age verification restrictions within the UK that have resulted from the Act.

122. With respect to VPNs being used to circumvent the Act's protections, government and Ofcom are keeping the issue under review. When debating the Bill, Parliament recognised that no regulatory regime is likely to be totally watertight and could not prevent a determined individual from accessing content online if they wished to do so.

123. These issues are not unique to the UK or to the Act, but are being faced by governments and regulators worldwide. For the UK to decide to tackle the use of VPNs and require services to block their use would necessitate significant extra territorial powers, and for the UK to regulate users from other countries. This would represent a significant shift in the UK government's stance.

DSIT000028 DSIT000029

124. Ofcom's Protection of Children Code for platforms **[SC/40], [SC/41]** does though clearly state that service providers should not publish content on their service which directs or encourages UK users to circumvent age assurance processes, for example by providing information about or links to a VPN.

Access to Individual Social Media Accounts

125. The Act does not give DSIT or Ofcom unfettered powers in the online safety space. DSIT is not able to obtain access to information communicated privately on a social media account or metadata about the use of that account. Direct access to these types of information would require a warrant or authorisation (respectively) under the Investigatory Powers Act 2016, neither of which DSIT is able to obtain.

126. Ofcom does have certain powers to obtain information from providers under the Act, but these can be used only for the purpose of exercising, or deciding whether to exercise, Ofcom's online safety functions. While Ofcom can require information

about an individual's use of a service, it would only be able to do so where this was required (and proportionate) for one of its regulatory functions in relation to online safety and would in most cases be limited pieces of information incidental to assessing, for example, a provider's systems and processes for addressing illegal content risks. Ofcom would be best placed to offer a more definitive answer on whether it would be able to provide the access which is sought, but DSIT does not consider that this is likely.

Additional Online Harms Work

127. The challenges presented by online harms cannot be addressed by the Act alone. It also requires effective collaboration between government, industry, academia and civil society. Therefore the government's response to online harms involves both legislative and non-legislative actions and using a broad toolkit allows DSIT to respond flexibly to the continually evolving threat.

128. Alongside its legislative work, DSIT is equipping both children and adults with the knowledge and skills to navigate the online world through our work on media literacy. Media literacy can help tackle a wide variety of online safety issues for all internet users, including children. It helps users understand that online actions have real-world consequences, enabling them to critically evaluate online information, and contributing to a respectful online environment.

129. DSIT engages regularly with stakeholders, including with social media platforms, to make clear that these services have a responsibility to keep their users safe and to deal with harmful content. DSIT has constructive relationships with the major platforms (Meta (formerly Facebook), TikTok, YouTube/Google, X) which have the largest reach in the UK. We engage with them on issues, emerging narratives, or events that may lead to a heightened risk to public safety or national security.

Reflection on Events

130. The Online Safety Act is a complex and far-reaching piece of legislation and the UK was one of the first countries in the world to introduce such legislation. However, it was always intended to be the starting point and the Secretary of State for DSIT has been clear that government will introduce additional legislation if there is a need to do so SC/38 DSIT000012. Monitoring and evaluation plays a key part in understanding how effective

the online safety regime is, and DSIT has developed a framework to monitor the implementation of the Act and evaluate the core outcomes. This framework draws on new and existing data to track specific metrics linked to the duties in the Act. Evaluation work will also assess the effectiveness of measures platforms have taken, for example implementing age assurance. The approach will track the effect of the online safety regime over time, as duties come into effect, and feed into a Post Implementation Review of the Act, as discussed further at paragraph 141 below.

131. As can be seen from the chronology set out above, it took a number of years to move from a Green Paper to the point now reached where the relevant provisions of the Act are being given effect. The Act introduces novel regulation in a complex, controversial and changing sector. Inevitably this means that there would always be a need for extensive consultation, Parliamentary and public debate, amendments and refinement. The effects of the Covid-19 pandemic, which altered the public's online habits, also had an effect. However, the speed of progress was more significantly influenced by political factors. In the period from October 2017 to Royal Assent, seven Secretaries of State have had responsibility for leading the legislative process in this area. Each one needed to understand the position reached when they were appointed and then decide on their priorities and approach in this immensely complex, politically charged, publicly exercising policy area.

132. The Act provided for a further period to implement and operationalise a brand new regulatory framework. Although Ofcom existed before the Act, its role on online safety was significantly expanded, requiring it to undertake preparatory work, such as the recruitment and training of staff. Furthermore, as mentioned above, it was required to consult on the various codes required by the Act and use the consultation responses to draft those codes. Under the Act Ofcom had an 18-month timeframe to finalise the illegal harms and child protection codes, and Ofcom met that deadline. The Act prioritised the implementation of the provisions relating to illegal content and child safety. Given the point at which Royal assent for the Act was obtained (26 October 2023), the implementation of these provisions couldn't have been expedited so as to be in place by 29 July 2024.

Improvements

133. The Inquiry has asked me to set out improvements that could be made within DSIT's areas of responsibility, to inform any recommendations that the Inquiry Chair makes in his Report.

134. The direction of future policy is properly a matter for democratically elected parliamentarians and government ministers to decide. As a civil servant, I do not think it would be appropriate for me to offer my opinion, in a public statement, on what changes should be made in the policy area in the future.

135. What I can say is that when policy is developed in this area, there will be a number of considerations that will be taken into account, such as the need to ensure children are protected from harmful online content, freedom of expression, the right to privacy, technological developments, and the economic and societal benefits that online access brings.

136. In order to keep pace with technological advancements and people's online habits, online safety policy will continue to adapt and evolve. The regulatory framework of the Act was always intended to be iterative and develop to combat new harms as they arise. DSIT Secretary of State has been clear that further online safety legislation will be needed; however, it is essential that government takes an evidenced based approach. That is why DSIT and Ofcom are working together on a monitoring and evaluation framework for the Online Safety Act. DSIT and Ofcom want to answer the following questions:

1. Are people – especially children – experiencing less harm online?

2. Are regulated services improving in how they protect users from online harms?

3. Are there unintended consequences of the new regulation that may require further action?

137. However, the government and Ofcom do not need to wait for the outcomes of the monitoring and evaluation framework to start making improvements in discrete areas. Ofcom is already consulting on additional measures **[SC/42]** that could be added to its Codes of Practice, including whether there is more that could be done around illegal content, tackling harms at source, and child safety. It is the government's **DSIT000007**

expectation that Ofcom will keep reviewing and amending its safety codes as more evidence emerges on effective safety measures.

138. The Act also includes an element of futureproofing, as any relevant updates to criminal law will be automatically captured under the regime. Consideration can also be given to making those updates into priority offences under the Act. If further categories of content are criminalised in future (for example, further types of violent content) then there would be opportunity to capture them under the Act.

139. The Secretary of State is particularly interested in exploring the question of the impact that social media usage has on children's mental health. The Act should increase protection for children from encountering harmful content, but there is academic debate about the extent to which children spending a material amount of time on social media can impact their mental health. That is why the last year our Secretary of State announced a new study into the impact of social media on young people's wellbeing and mental health, which will be key evidence to inform the future direction of this work. It will be published in due course.

140. DSIT is also aware of the need to ensure that legislation is keeping pace with technological advancements. The Act is tech neutral (it applies to any technology or service in scope of the Act) and does apply to a wide range of services; however, the government is keeping under review the risks that AI could pose to users and has already proposed new criminal offences, for example new AI sexual abuse offences to protect children from predators generating AI images.

141. Additionally, section 178 of the Act requires the Secretary of State to review the effectiveness of the regime two to five years after all of part 3 of the Act is in force. The exact dates of when this review will be conducted is dependent on the ongoing implementation of the Act. These timescales are set out in primary legislation and reflect the need for the regulatory framework to be operational for some time so that there is sufficient data available to measure its success. Once the review has been conducted a report setting out the findings must be published and laid in Parliament.

Statement of Truth

I believe that the facts stated in this witness statement are true. I understand that proceedings many 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.

Signature

Signed:_____

Dated: 03 September 2025